Swing Barrier

User Manual

Legal Information

About this Document

- This Document includes instructions for using and managing the Product. Pictures, charts, images and all other information hereinafter are for description and explanation only.
- The information contained in the Document is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version of the Document at the Hikvision website (***https://www.hikvision.com***). Unless otherwise agreed, Hangzhou Hikvision Digital Technology Co., Ltd. or its affiliates (hereinafter referred to as "Hikvision") makes no warranties, express or implied.
- Please use the Document with the guidance and assistance of professionals trained in supporting the Product.

About this Product

- This product can only enjoy the after-sales service support in the country or region where the purchase is made.
- If the product you choose is a video product, please scan the following QR code to obtain the "Initiatives on the Use of Video Products", and read it carefully.

Acknowledgment of Intellectual Property Rights

- Hikvision owns the copyrights and/or patents related to the technology embodied in the Products described in this Document, which may include licenses obtained from third parties.
- Any part of the Document, including text, pictures, graphics, etc., belongs to Hikvision. No part of this Document may be excerpted, copied, translated, or modified in whole or in part by any means without written permission.
- HIKVISION and other Hikvision's trademarks and logos are the properties of Hikvision in various jurisdictions.
- Other trademarks and logos mentioned are the properties of their respective owners.

LEGAL DISCLAIMER

- TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THIS DOCUMENT AND THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, ARE PROVIDED "AS IS" AND "WITH ALL FAULTS AND ERRORS". HIKVISION MAKES NO WARRANTIES, EXPRESS OR

IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THE PRODUCT BY YOU IS AT YOUR OWN RISK. IN NO EVENT WILL HIKVISION BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA, CORRUPTION OF SYSTEMS, OR LOSS OF DOCUMENTATION, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY, OR OTHERWISE, IN CONNECTION WITH THE USE OF THE PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSS.

- YOU ACKNOWLEDGE THAT THE NATURE OF THE INTERNET PROVIDES FOR INHERENT SECURITY RISKS, AND HIKVISION SHALL NOT TAKE ANY RESPONSIBILITIES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER-ATTACK, HACKER ATTACK, VIRUS INFECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.
- YOU AGREE TO USE THIS PRODUCT IN COMPLIANCE WITH ALL APPLICABLE LAWS, AND YOU ARE SOLELY RESPONSIBLE FOR ENSURING THAT YOUR USE CONFORMS TO THE APPLICABLE LAW. ESPECIALLY, YOU ARE RESPONSIBLE, FOR USING THIS PRODUCT IN A MANNER THAT DOES NOT INFRINGE ON THE RIGHTS OF THIRD PARTIES, INCLUDING WITHOUT LIMITATION, RIGHTS OF PUBLICITY, INTELLECTUAL PROPERTY RIGHTS, OR DATA PROTECTION AND OTHER PRIVACY RIGHTS. YOU SHALL NOT USE THIS PRODUCT FOR ANY PROHIBITED END-USES, INCLUDING THE DEVELOPMENT OR PRODUCTION OF WEAPONS OF MASS DESTRUCTION, THE DEVELOPMENT OR PRODUCTION OF CHEMICAL OR BIOLOGICAL WEAPONS, ANY ACTIVITIES IN THE CONTEXT RELATED TO ANY NUCLEAR EXPLOSIVE OR UNSAFE NUCLEAR FUEL-CYCLE, OR IN SUPPORT OF HUMAN RIGHTS ABUSES.
- IN THE EVENT OF ANY CONFLICTS BETWEEN THIS DOCUMENT AND THE APPLICABLE LAW, THE LATTER PREVAILS.

Data Protection

- To protect data, the development of Hikvision Products incorporates privacy by design principles. For example, for Products with facial recognition features, biometrics data is stored in your Products with encryption method; for fingerprint Products, only fingerprint template will be saved, which is impossible to reconstruct a fingerprint image.
- As a data controller/processor, you may process personal data, including collection, storage, use, processing, disclosure, deletion, etc. You are advised to pay attention to and comply with applicable laws and regulations related to the protection of personal data, including without limitation, conducting security controls to safeguard personal data, such as, implementing reasonable administrative and physical security controls, conduct periodic reviews and the assessments of the effectiveness of your security controls.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help

This equipment should be installed and operated with a minimum distance 20cm between the radiator and your body.

FCC Conditions

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, RE Directive 2014/53/EU,the RoHS Directive 2011/65/EU

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see:www.recyclethis.info

Safety Instruction

These instructions are intended to ensure that user can use the product correctly to avoid danger or property loss.

The precaution measure is divided into Dangers and Cautions:

Dangers: Neglecting any of the warnings may cause serious injury or death.

Cautions: Neglecting any of the cautions may cause injury or equipment damage.

⚠	⚠
Dangers: Follow these safeguards to prevent serious injury or death.	**Cautions:** Follow these precautions to prevent potential injury or material damage.

⚠ Danger:

- In the use of the product, you must be in strict compliance with the electrical safety regulations of the nation and region.
- The equipment must be connected to an earthed mains socket-outlet.
- Shock hazard! Disconnect all power sources before maintenance.
- Do not touch the bare metal contacts of the inlets after the circuit breaker is turned off. Electricity still exists.
- ϟ indicates hazardous live and the external wiring connected to the terminals requires installation by an instructed person.
- Keep body parts away from fan blades. Disconnect the power source during servicing.
- Keep body parts away from motors. Disconnect the power source during servicing.
- To prevent possible hearing damage, do not listen at high volume levels for long periods.
- All the electronic operation should be strictly compliance with the electrical safety regulations, fire prevention regulations and other related regulations in your local region.
- Do not connect several devices to one power adapter as adapter overload may cause over-heat or fire hazard.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.

  If the top caps should be open and the device should be powered on for maintenance, make sure:

  1. Power off the fan to prevent the operator from getting injured accidentally.
  2. Do not touch bare high-voltage components.
  3. Make sure the switch’s wiring sequence is correct after maintenance.
- Please make sure that the power has been disconnected before you wire, install or dismantle the device.
- When the product is installed on wall or ceiling, the device shall be firmly fixed.
- If smoke, odors or noise rise from the device, turn off the power at once and unplug the power cable, and then please contact the service center.

- Do not ingest battery, Chemical Burn Hazard.
  This product contains a coin/button cell battery. If the coin/button cell battery is swallowed, it can cause severe internal burns in just 2 hours and can lead to death.
  Keep new and used batteries away from children. If the battery compartment does not close securely, stop using the product and keep it away from children. If you think batteries might have been swallowed or placed inside any part of the body, seek immediate medical attention.
- If the product does not work properly, please contact your dealer or the nearest service center. Never attempt to disassemble the device yourself. (We shall not assume any responsibility for problems caused by unauthorized repair or maintenance.)

⚠ Cautions:

- The equipment shall not be exposed to dripping or splashing and that no objects filled with liquids, such as vases, shall be placed on the equipment.
- Ensure correct wiring of the terminals for connection to an AC mains supply.
- The equipment has been designed, when required, modified for connection to an IT power distribution system.
- + identifies the positive terminal(s) of equipment which is used with, or generates direct current. + identifies the negative terminal(s) of equipment which is used with, or generates direct current.
- No naked flame sources, such as lighted candles, should be placed on the equipment.
- This equipment is suitable for mounting on concrete or other non-combustible surface only.
- Install the equipment according to the instructions in this manual.
- To prevent injury, this equipment must be securely attached to the floor/wall in accordance with the installation instructions.
- Stainless steel may be corroded in some circumstances. You need to clean and care the device by using the stainless steel cleaner. It is suggested to clean the device every month.
- Do not drop the device or subject it to physical shock, and do not expose it to high electromagnetism radiation. Avoid the equipment installation on vibrations surface or places subject to shock (ignorance can cause equipment damage).
- Do not place the device in extremely hot (refer to the specification of the device for the detailed operating temperature), cold, dusty or damp locations, and do not expose it to high electromagnetic radiation.
- The device cover for indoor use shall be kept from rain and moisture.
- Exposing the equipment to direct sun light, low ventilation or heat source such as heater or radiator is forbidden (ignorance can cause fire danger).
- Do not aim the device at the sun or extra bright places. A blooming or smear may occur otherwise (which is not a malfunction however), and affecting the endurance of sensor at the same time.
- Please use the provided glove when open up the device cover, avoid direct contact with the device cover, because the acidic sweat of the fingers may erode the surface coating of the device cover.
- Please use a soft and dry cloth when clean inside and outside surfaces of the device cover, do not use alkaline detergents.

- Please keep all wrappers after unpack them for future use. In case of any failure occurred, you need to return the device to the factory with the original wrapper. Transportation without the original wrapper may result in damage on the device and lead to additional costs.
- Improper use or replacement of the battery may result in hazard of explosion. Replace with the same or equivalent type only. Dispose of used batteries according to the instructions provided by the battery manufacturer.
- Biometric recognition products are not completely applicable to anti-spoofing environments. If you require a higher security level, use multiple authentication modes.
- Do not stay in the lane when the device is rebooting.
- RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTIONS.
- SUITABLE FOR MOUNTING ON CONCRETE OR OTHER NON-COMBUSTIBLE SURFACE ONLY.
- The instructions shall require connection of the equipment protective earthing conductor to the installation protective earthing conductor.

Available Models

Product Name	Model	Description
Swing Barrier	DS-K3B801BX-L	Left Pedestal
	DS-K3B801BX-M	Middle Pedestal
	DS-K3B801BX-R	Right Pedestal

Contents

Chapter 1 Overview 1

1.1 Introduction 1

1.2 Main Features 1

Chapter 2 System Wiring 3

Chapter 3 Installation 5

3.1 Disassemble before Installation 5

3.2 Install Pedestals 8

Chapter 4 General Wiring 10

4.1 Components Introduction 10

4.2 Wiring Electric Supply 13

4.3 Wire Interconnecting Cable 15

4.4 Wire Network Switch 15

4.5 Terminal Description 16

4.5.1 Main Lane Control Board Terminal Description 16

4.5.2 Sub Lane Control Board Terminal Description 17

4.5.3 Access Control Board Terminal Description 18

4.5.4 Main Extended Interface Board Terminal Description 20

4.5.5 Sub Extended Interface Board Terminal Description 22

4.5.6 Card Reader Board Terminal Description 23

4.5.7 Lane Status Indicator Board 23

4.5.8 Wiring Diagram 25

4.5.9 RS-485 Wiring 26

4.5.10 Face Recognition Module Wiring 26

Chapter 5 Device Settings 29

5.1 Set Study Mode 29

5.2 Pair Keyfob 31

5.3 Initialize Device 33

Chapter 6 Activation 34

6.1 Activate via SADP 34

6.2 Activate Device via Client Software 35

6.3 Activate via Web Browser 36

Chapter 7 Operation via Web Browser 37

7.1 Login 37

7.2 Web Wizard 37

7.2.1 Time Settings 37

7.2.2 Administrator Settings 38

7.3 Overview 38

7.4 Person Management 39

7.5 Search Event 41

7.6 Configuration 43

7.6.1 View Device Information 43

7.6.2 Set Time 43

7.6.3 Set DST 44

7.6.4 Change Administrator's Password 44

7.6.5 Online Users 44

7.6.6 View Device Arming/Disarming Information 45

7.6.7 Network Settings 45

7.6.8 Set Audio Parameters 47

7.6.9 Event Linkage 47

7.6.10 Access Control Settings 48

7.6.11 Turnstile 53

7.6.12 Card Settings 57

7.6.13 Set Privacy Parameters 58

7.6.14 Set Smart Parameters 58

7.6.15 Prompt Schedule 59

7.6.16 Upgrade and Maintenance 61

7.6.17 Device Debugging 62

7.6.18 Component Status 63

7.6.19 Log Query 64

7.6.20 Certificate Management 64

Chapter 8 Client Software Configuration 66

8.1 Configuration Flow of Client Software 66

8.2 Device Management 66

8.2.1 Add Device 67

8.2.2 Reset Device Password 69

8.2.3 Manage Added Devices 70

8.3 Group Management 71

8.3.1 Add Group 71

8.3.2 Import Resources to Group 72

8.4 Person Management 72

8.4.1 Add Organization 72

8.4.2 Configure Basic Information 73

8.4.3 Issue a Card by Local Mode 73

8.4.4 Upload a Face Photo from Local PC 75

8.4.5 Take a Photo via Client 76

8.4.6 Collect Face via Access Control Device 77

8.4.7 Collect Fingerprint via Client 78

8.4.8 Collect Fingerprint via Access Control Device 79

8.4.9 Configure Access Control Information 80

8.4.10 Customize Person Information 81

8.4.11 Configure Resident Information 82

8.4.12 Configure Additional Information 82

8.4.13 Import and Export Person Identify Information 83

8.4.14 Import Person Information 83

8.4.15 Import Person Pictures 84

8.4.16 Export Person Information 84

8.4.17 Export Person Pictures 85

8.4.18 Get Person Information from Access Control Device 85

8.4.19 Move Persons to Another Organization 86

8.4.20 Issue Cards to Persons in Batch 86

8.4.21 Report Card Loss 87

8.4.22 Set Card Issuing Parameters 87

8.5 Configure Schedule and Template 88

8.5.1 Add Holiday 88

8.5.2 Add Template 89

8.6 Set Access Group to Assign Access Authorization to Persons 90

8.7 Configure Advanced Functions 93

8.7.1 Configure Device Parameters 93

8.7.2 Configure Remaining Open/Closed 99

8.7.3 Configure Multi-Factor Authentication 100

8.7.4 Configure Custom Wiegand Rule 103

8.7.5 Configure Card Reader Authentication Mode and Schedule 104

8.7.6 Configure First Person In 106

8.7.7 Configure Anti-Passback 107

8.7.8 Configure Device Parameters 108

8.8 Configure Linkage Actions for Access Control 109

8.8.1 Configure Client Actions for Access Event 109

8.8.2 Configure Device Actions for Access Event 110

8.8.3 Configure Device Actions for Card Swiping 111

8.9 Door Control 112

8.9.1 Control Door Status ... 113

8.9.2 Check Real-Time Access Records ... 114

Appendix A. Tips for Scanning Fingerprint ... 116

Appendix B. DIP Switch ... 118

B.1 DIP Switch Description ... 118

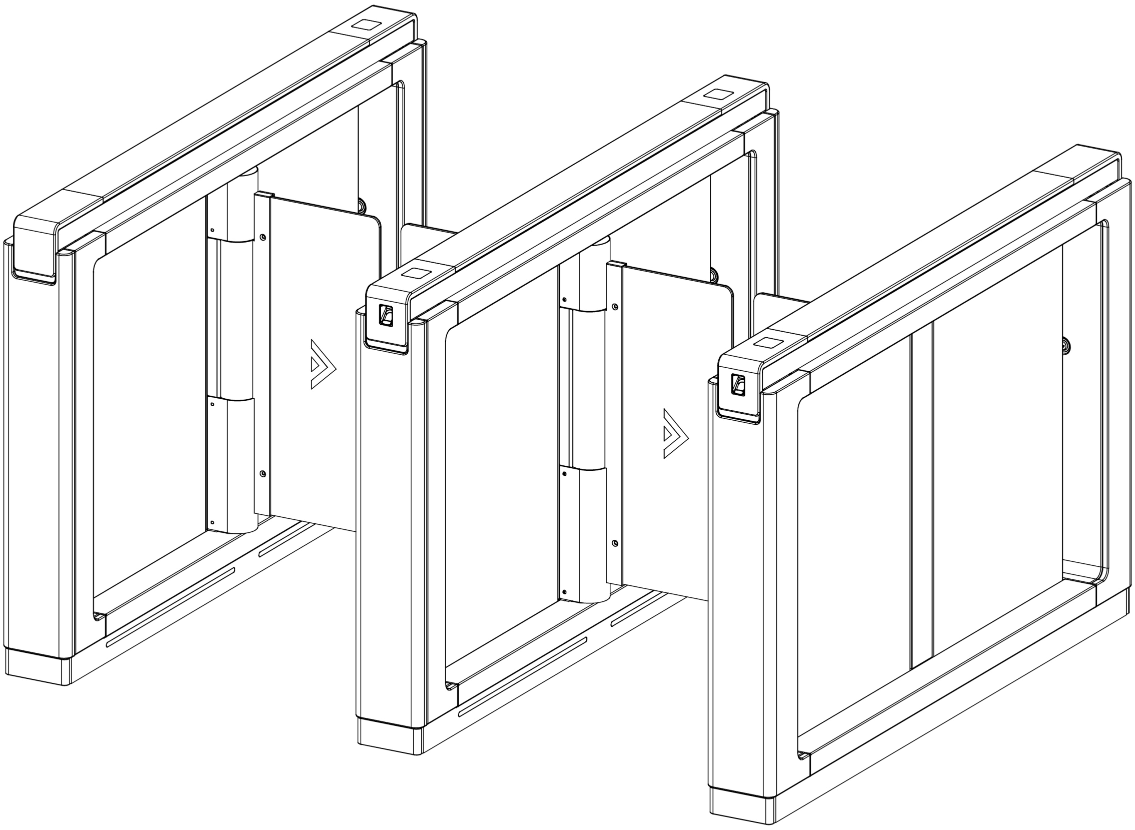
B.2 DIP Switch Corresponded Functions ... 118

Appendix C. Error Code Description ... 119

Appendix D. Communication Matrix and Device Command ... 121

Chapter 1 Overview

1.1 Introduction



The swing barrier with two barriers and 24 pair of IR lights is designed to detect unauthorized entrance or exit. By adopting the swing barrier integrated with the access control system, person should authenticate to pass through the lane via swiping IC or ID card, scanning QR code, etc. It is widely used in attractions, stadiums, construction sites, residences, etc.

1.2 Main Features

- 32-bit high-speed processor
- TCP/IP network communication
  The communication data is specially encrypted to relieve the concern of privacy leak.
- Permissions validation and anti-tailgating
- Remaining open/closed mode selectable
- Bidirectional (Entering/Exiting) lane
  The barrier opening and closing speed can be configured according to the visitor flow.

- The barrier will be locked or stop working when people are nipped
- Anti-forced-accessing
  The barrier will be locked automatically without open-barrier signal.
- Self-detection, Self-diagnostics, and automatic alarm
- Audible and visual alarm will be triggered when detecting intrusion, tailgating, reverse passing, and climbing over barrier
- IP conflict detection
- Remote control and management
- Online/offline operation
- LED indicates the entrance/exit and light bar indicates passing status
- Barrier remains open when powered down
- Fire alarm passing
  When the fire alarm is triggered, the barrier will be open automatically for emergency evacuation
- Valid passing duration settings
  System will cancel the passing permission if a person does not pass through the lane within the valid passing duration
- Opens/Closes barrier according to the schedule template

Chapter 2 System Wiring

The preparation before installation and wiring.

Steps

1. Draw a central line on the installation surface of the left or right pedestal.
2. Draw other parallel lines for installing the other pedestals.

Note

The distance between the nearest two line is L+190 mm. L represents the lane width.

3. Slotting on the installation surface and dig installation holes according to the hole position diagram.

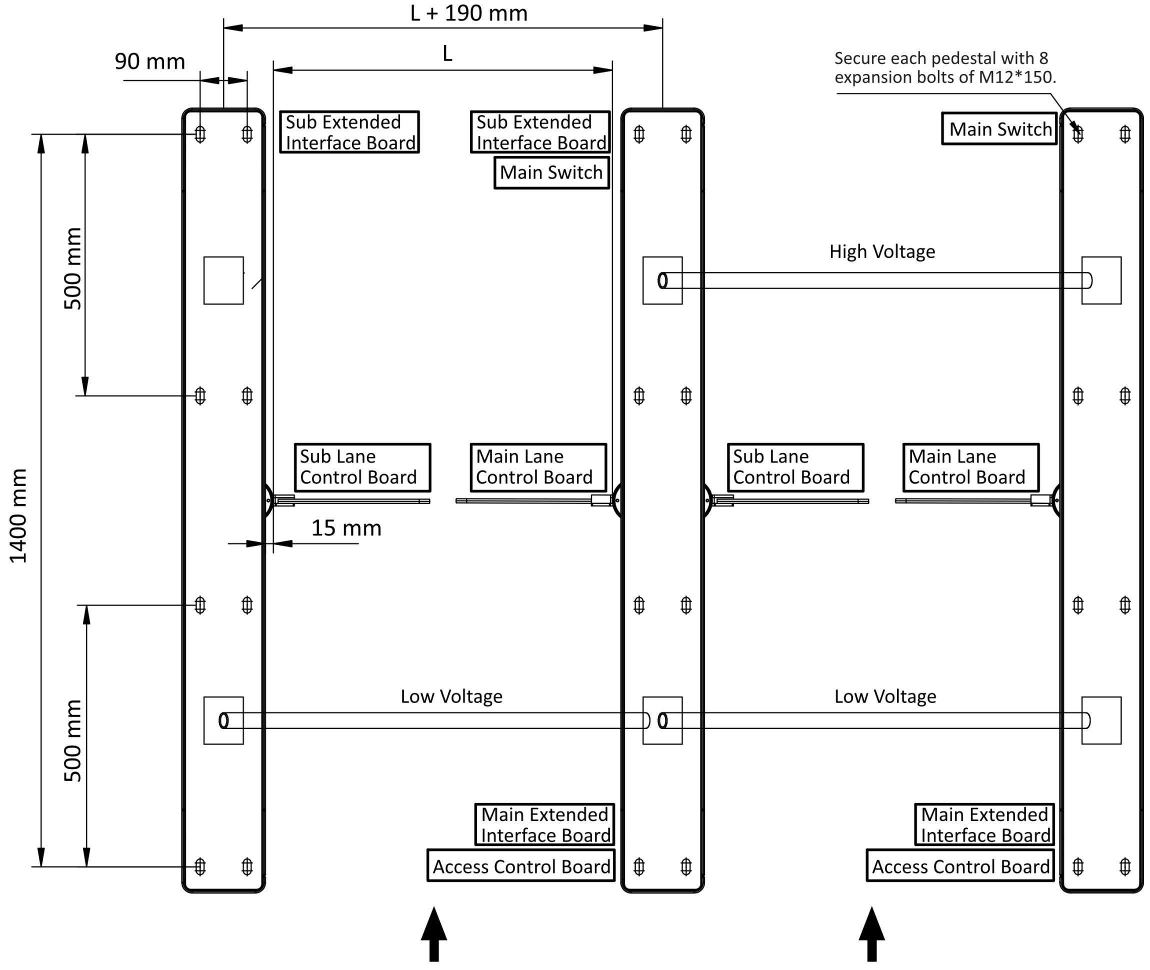


Figure 2-1 Hole Position Diagram

4. Bury cables. Each lane buries 1 low voltage cable and 1 high voltage cable. For details, see the system wiring diagram above.

Note

- High voltage: AC power input
- Low voltage: interconnecting cables
- The supplied interconnecting cables are 5.5 m in length.
- The suggested inner diameter of the low voltage conduit is larger than 30 mm.
- If you want to bury both of the AC power cord and the low voltage cable at the entrance, the two cables should be in separated conduits to avoid interference.
- If more peripherals are required to connect, you should increase the conduit diameter or bury another conduit for the external cables.
- The external AC power cord should be double-insulated.
- The network cable must be CAT5e or the network cable has better performance. And the suggested network cable length should be less than 100 m.

Chapter 3 Installation

3.1 Disassemble before Installation

Before installation, you should disassemble the pedestal and remove some screws.

Before You Start

- Keep the disassembled components and screws.
- You should prepare the following tools to disassemble the pedestal: 1. Pedestal Key (supplied); 2. Allen Wrench (2.5 mm); 3. Allen Wrench (3 mm); 4. Allen Wrench (4 mm).

Steps

1. Use the pedestal key to open the front and back components.

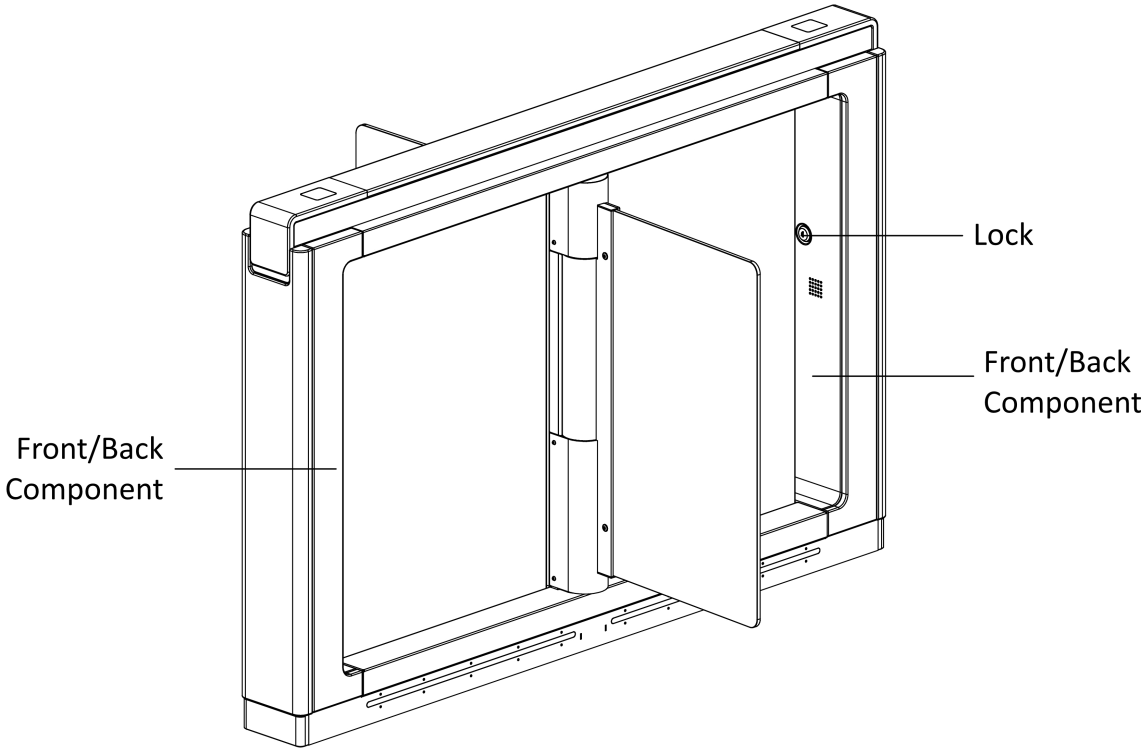


Figure 3-1 Lock Position

2. Use the Allen wretch (4 mm) to loosen the 2 screws (M5 × 25) at the top of the device and remove the components carefully.

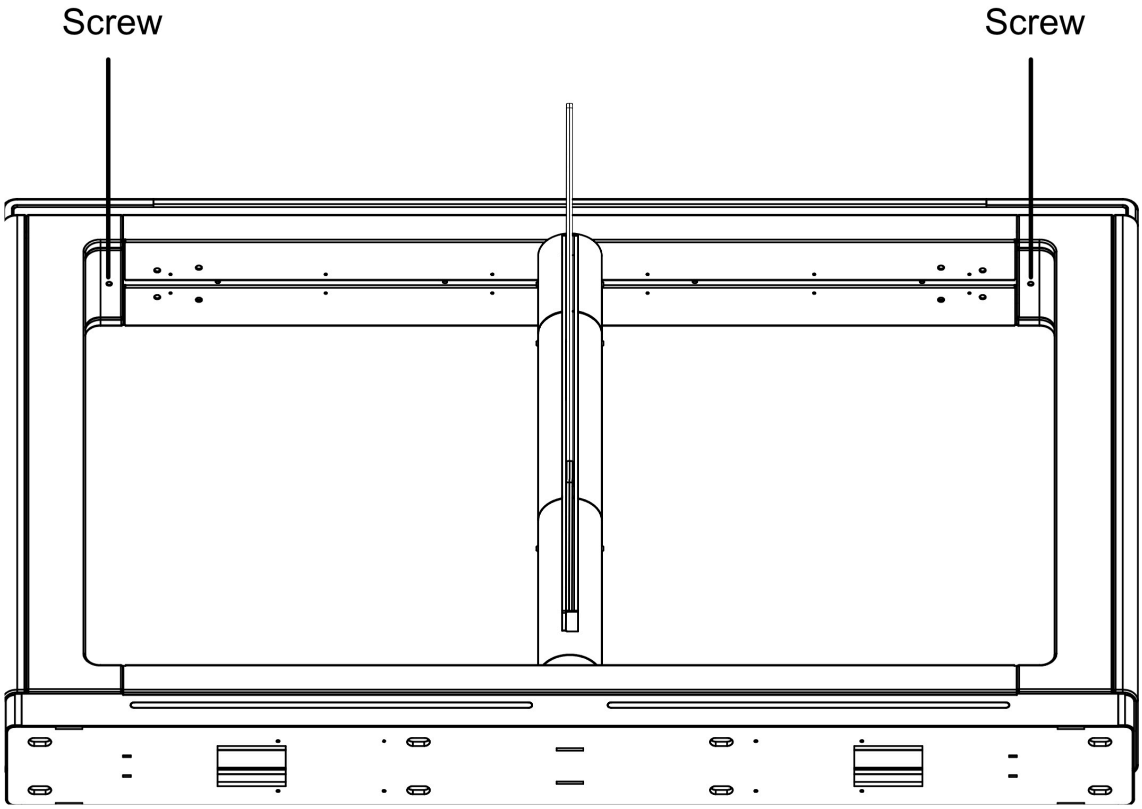


Figure 3-2 Front/Back Component Screw

3. Use the Allen wretch (4 mm) to loosen the 2 screws (M5 × 12) at the front or back of the pedestal base and remove the side base cover slowly.

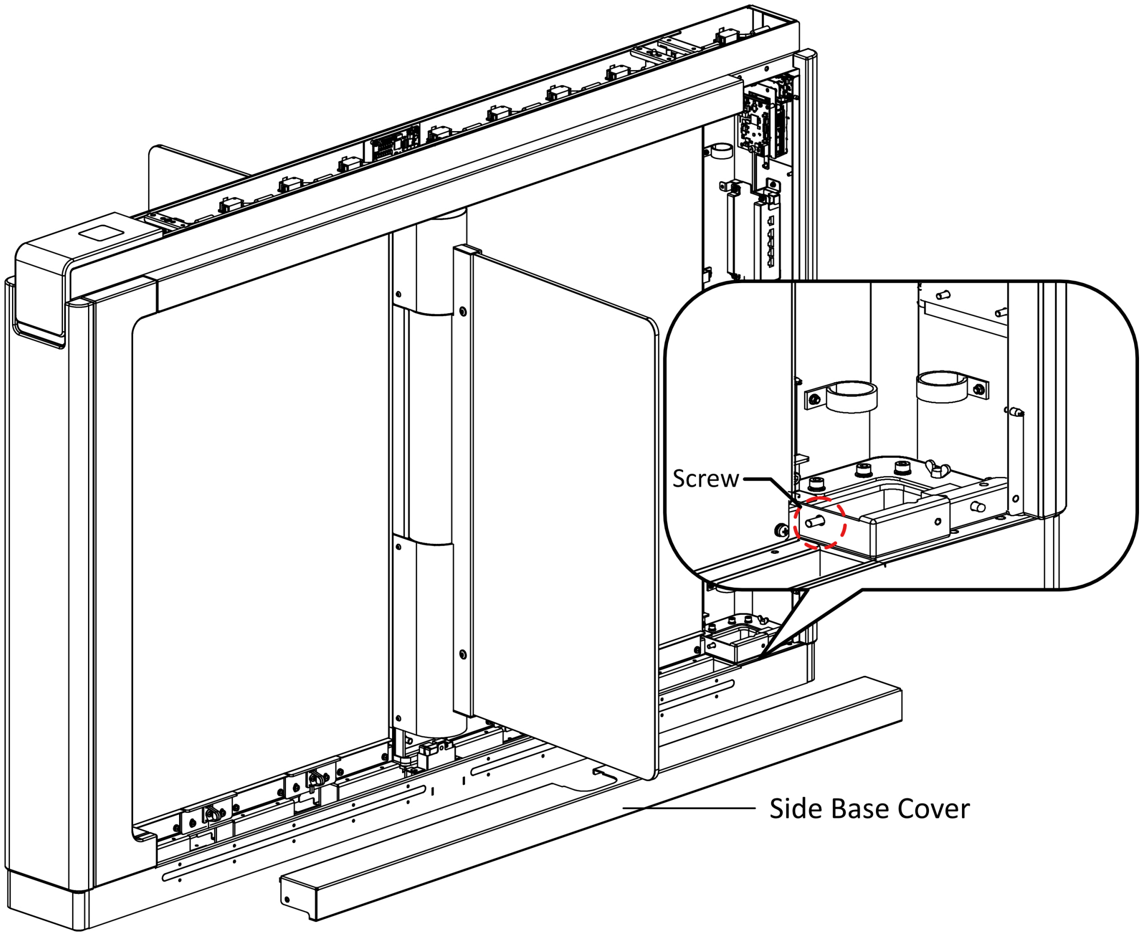


Figure 3-3 Loosen Side Base Screw

4. Use the Allen wretch (2.5 mm) to loosen the 4 screws (M4 × 8) and remove the motor bottom cover.

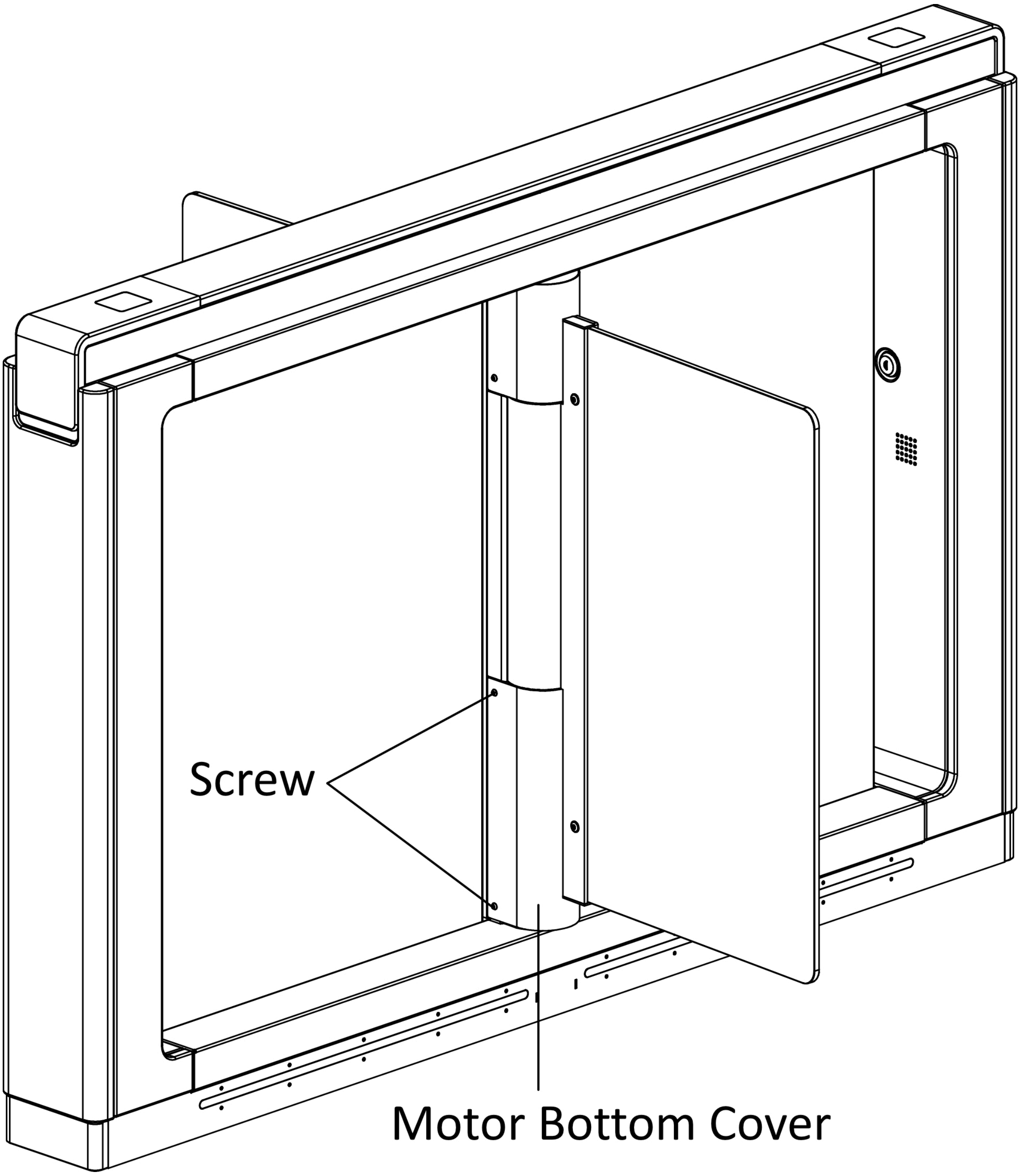


Figure 3-4 Motor Bottom Cover

3.2 Install Pedestals

Before You Start

Prepare for the installation tools, check the device and the accessories, and clear the installation base.

Steps

Note

- The device should be installed on the concrete surface or other non-flammable surfaces.
- The dimension is as follows.

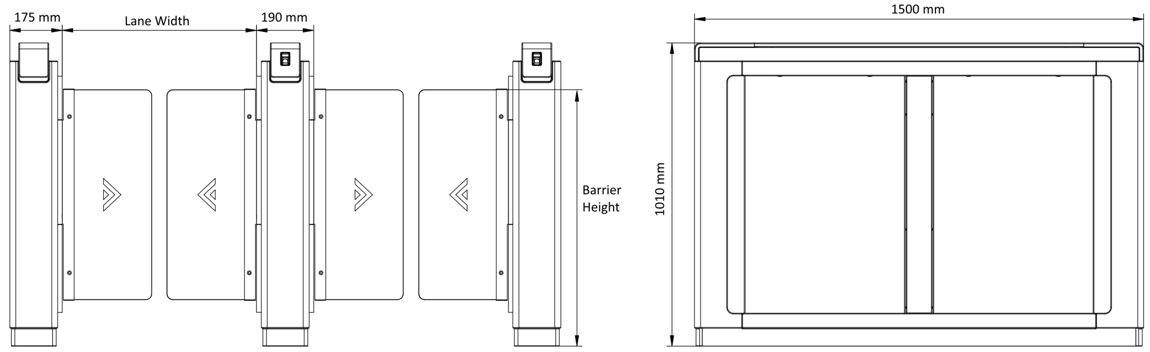


Figure 3-5 Dimension

1. Prepare for the installation tools, check the components, and prepare for the installation base.
2. Drill holes on the ground according to the installation holes on the pedestals and insert the expansion sleeves.
3. According to the entrance and exit marks on the pedestals, move the pedestals to the corresponded positions.

   Note

   Make sure the installation holes on the pedestals and the base are aligned with each other.
4. Secure each pedestal with 8 expansion bolts.

   Note

   Do not immerse the pedestal in the water. In special circumstances, the immersed height should be no more than 150 mm.
5. After installation, assemble the components and screws back to the pedestal in reverse order (except for protective sheets).

Chapter 4 General Wiring

4.1 Components Introduction

By default, basic components of the turnstile are connected well. The pedestals can communicate by wiring the interconnecting cables. And the turnstile supports wiring the AC electric supply for the whole system's power supply.

Note

The voltage fluctuation of the electric supply is between 100 VAC and 220 VAC, 50 to 60 Hz.

The picture displayed below describes each component's position on the turnstile.

Note

The diagram is for reference only.

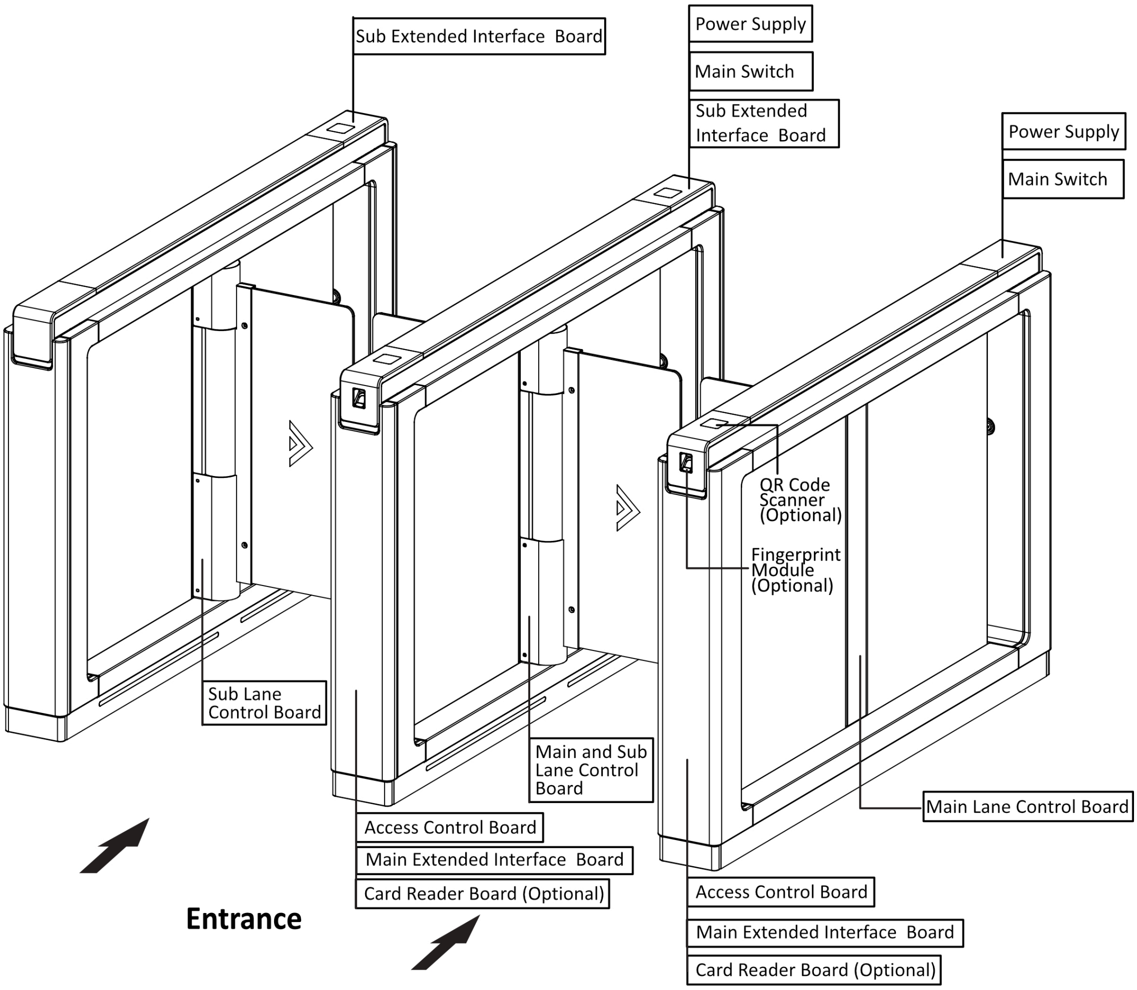

Sub Extended Interface Board
Power Supply
Main Switch
Sub Extended Interface Board
Power Supply
Main Switch
QR Code Scanner (Optional)
Fingerprint Module (Optional)
Sub Lane Control Board
Main and Sub Lane Control Board
Main Lane Control Board
Access Control Board
Main Extended Interface Board
Card Reader Board (Optional)
Access Control Board
Main Extended Interface Board
Card Reader Board (Optional)
Entrance

Figure 4-1 Components Diagram

The picture displayed below describes the serial port on the entrance and exit direction.

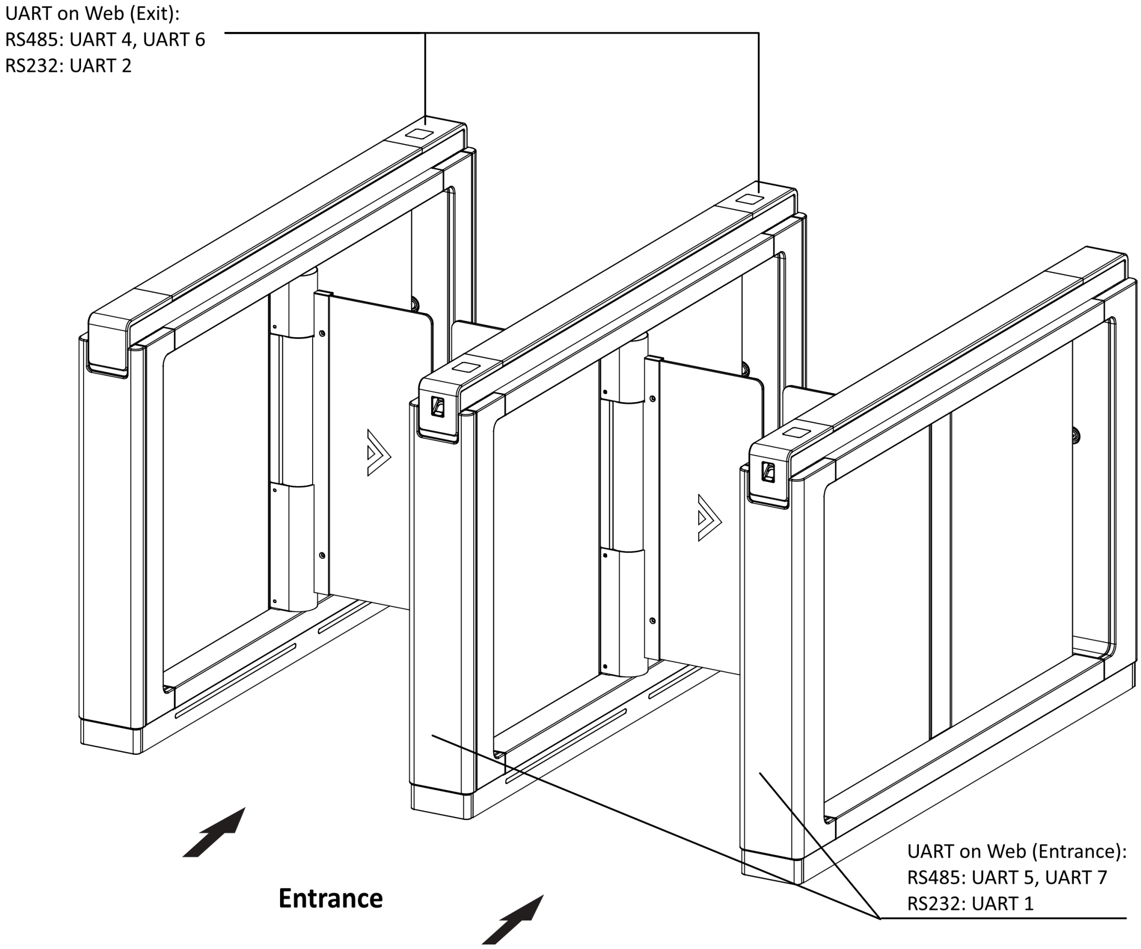


Figure 4-2 Serial Port

The picture displayed below describes the IR sending/receiving module and their corresponding number on the pedestal.

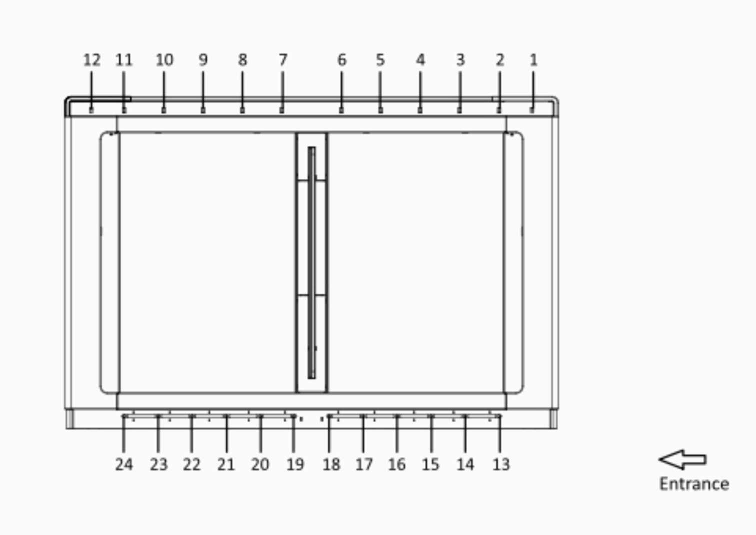


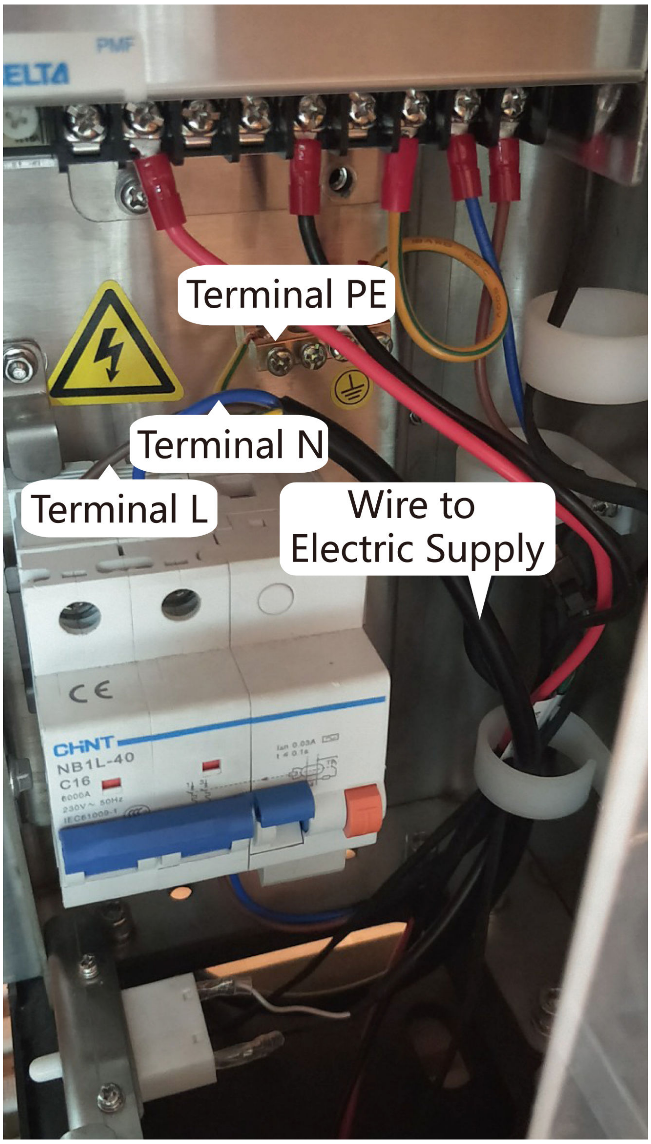
Figure 4-3 IR Sending/Receiving Module Position

Note

Standing at the entrance position in the lane, the IR modules on your left are the IR sending modules, the ones on your right are the IR receiving modules.

4.2 Wiring Electric Supply

Wire electric supply with the switch in the pedestal. Terminal L and terminal N are on the switch, while terminal PE should connect to a ground wire (yellow and green wire).



Note

- The cable bare part should be no more than 8 mm. It is suggested that you can immerse the bare part into the liquid tin. If possible, wear an insulation cap at the end of the bare cable. Make sure there’s no bare copper or cable after the wiring.
- The Terminal L and the Terminal N cannot be wired reversely. Do not wire the input and output terminal reversely.
- To avoid people injury and device damage, when testing, the ground resistance of the equipotential points should not be larger than 2 Ω。
- Use the device in conjunction with an UPS.

4.3 Wire Interconnecting Cable

You should use interconnecting cables to connect the main lane board and the sub lane board for components communication.

The picture displayed below describes the cable hole's position on the pedestals.

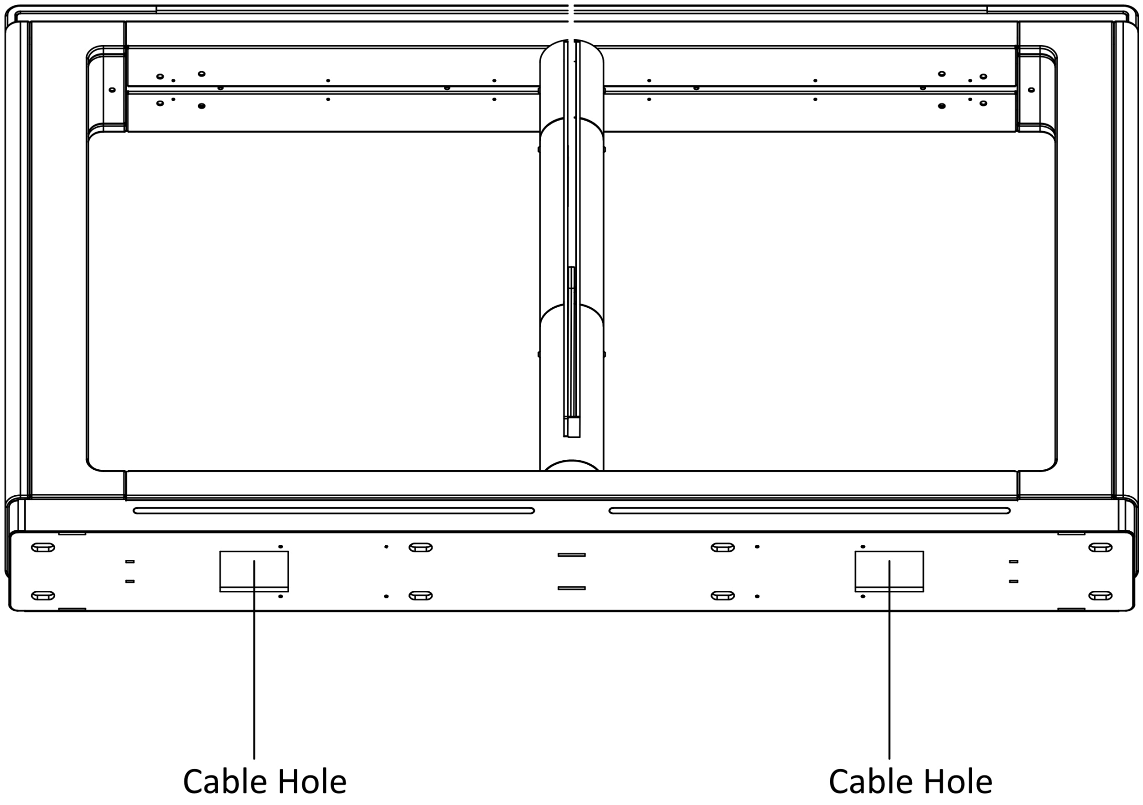


Figure 4-4 Cable Hole of Interconnecting Cable

For interconnecting cable wiring, refer to ***Wiring Diagram*** .

4.4 Wire Network Switch

Connect the network cable and the network switch.

Steps

Note

The device do not support the PoE network switch. Connecting with the PoE network switch may damage the control board.

1. Open the side cover of the pedestal.

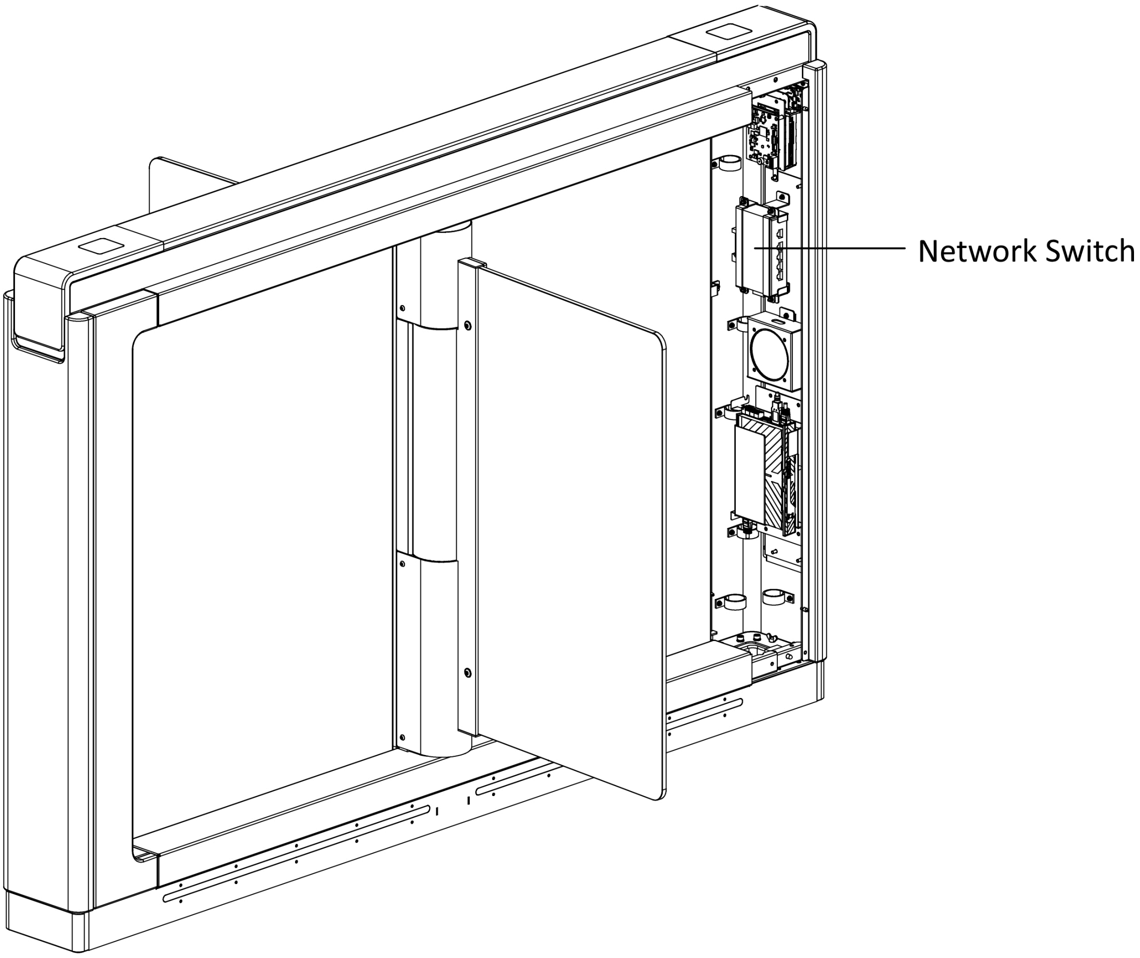


Figure 4-5 Network Switch Position

2. Lead out 12 V power supply from the main switch and connect it to the network switch's power interface.
3. Connect the network cable with the network switch.

4.5 Terminal Description

The lane controller contains main lane controller and sub lane controller, which controls the IR beams, motor, and other components' work.

4.5.1 Main Lane Control Board Terminal Description

The main lane control board contains power supply interface, supercapacitor interface, brake interface, motor drive interface, light board interface, motor encoder interface, door open position detection interface, debug port, lane communication interface, interconnecting interface, and DIP switch (reserved).

The picture displayed below is the main lane control board diagram.

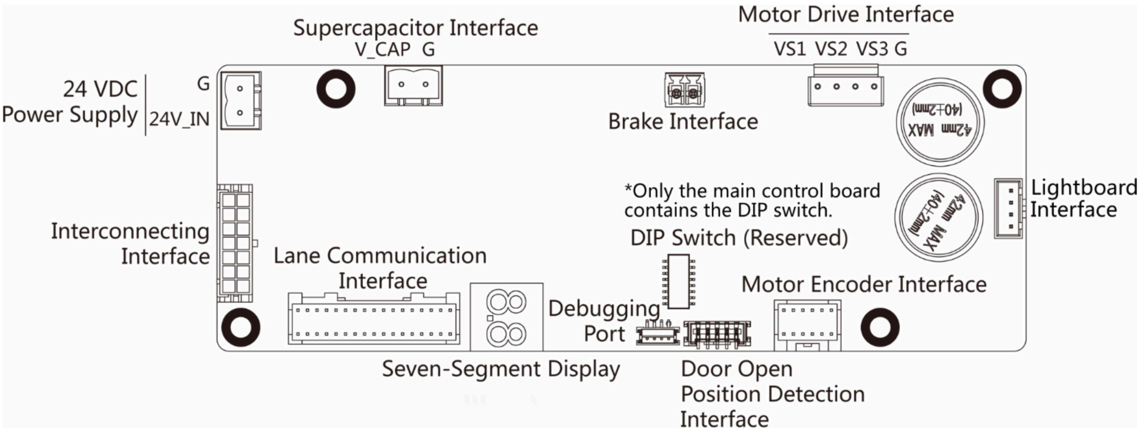


Figure 4-6 Main Lane Control Board

4.5.2 Sub Lane Control Board Terminal Description

The sub lane control board contains power supply interface, supercapacitor interface, brake interface, motor drive interface, light board interface, motor encoder interface, door open position detection interface, debug port, lane communication interface, and interconnecting interface.

The picture displayed below is the sub lane control board diagram.

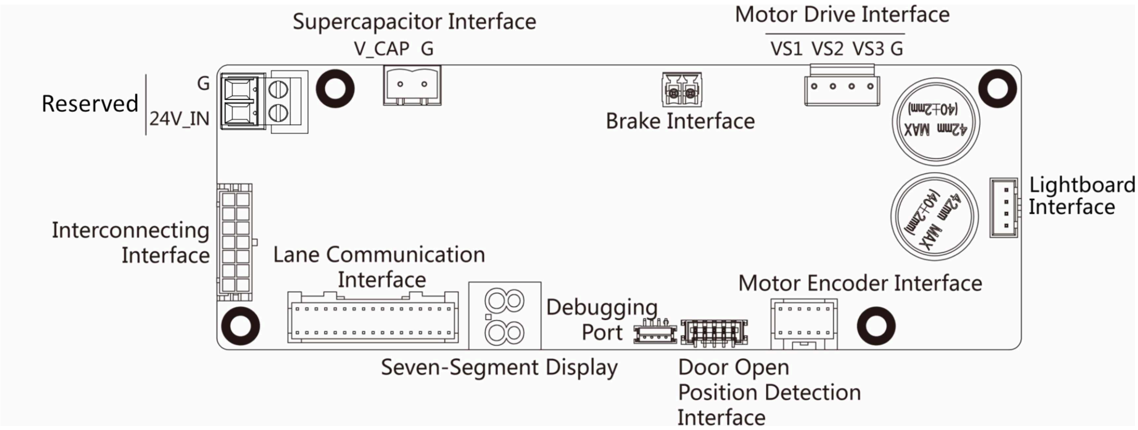


Figure 4-7 Sub Lane Control Board

4.5.3 Access Control Board Terminal Description

Access control board is mainly used for authority identification in places with high security levels such as public security or judicial place, external device accessing, and communication with the upper platform and lane controller.

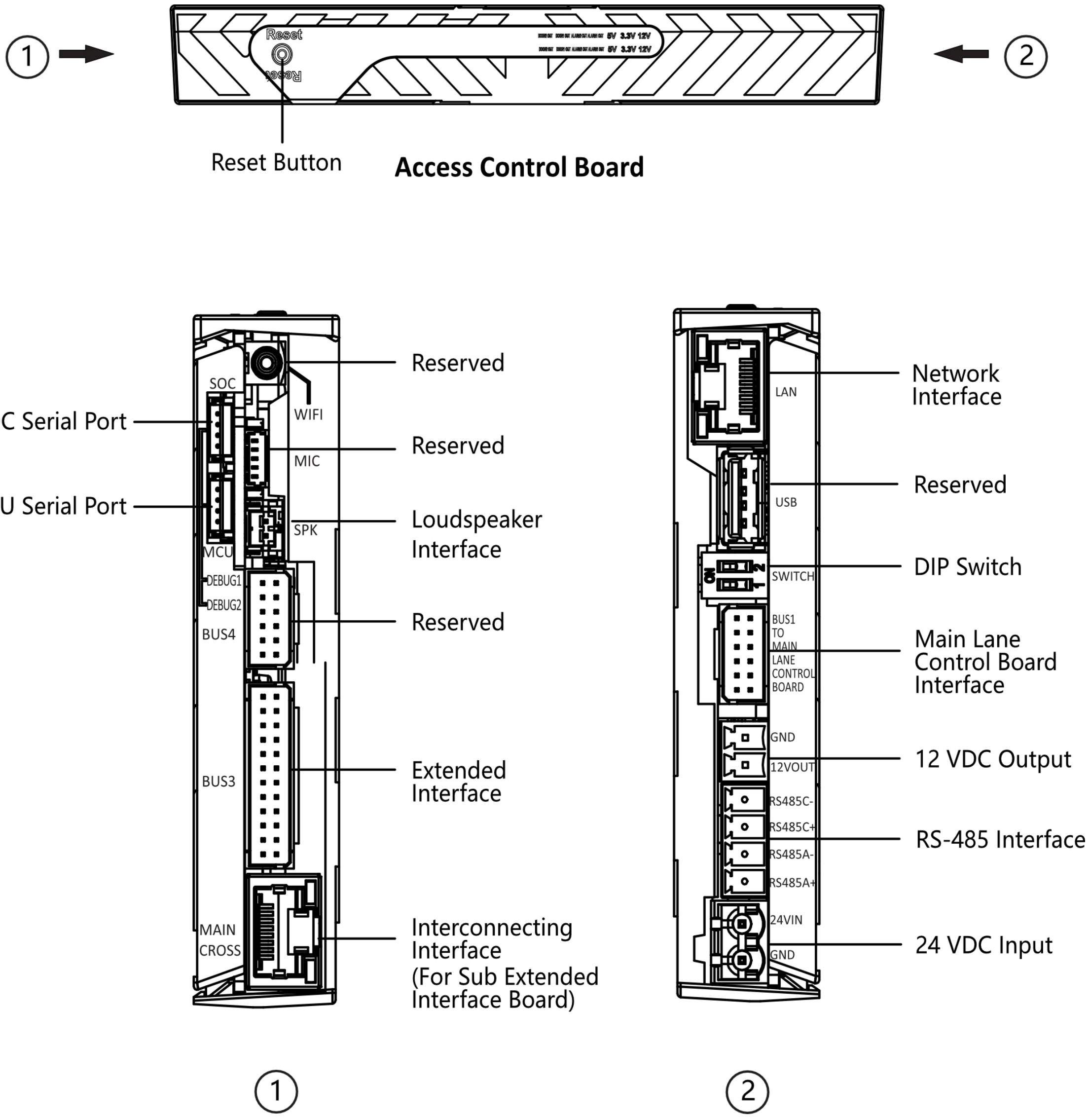


Figure 4-8 Access Control Board

Note

- RS-485A corresponds to UART 5 on web and is for QR code scanner connection at entrance by default; RS-485C corresponds to UART 7 on web and is for card reader connection at entrance by default.
- The SOC and MCU serial port are for maintenance and debugging use only.
- Press the Reset button for 5 s and the device will start to restore to factory settings.
- The DIP switch is for study mode setting and keyfob paring. For detailed information about the DIP switch, see *DIP Switch Description*.

The wiring diagram of extended interface of access control board is shown as follows.

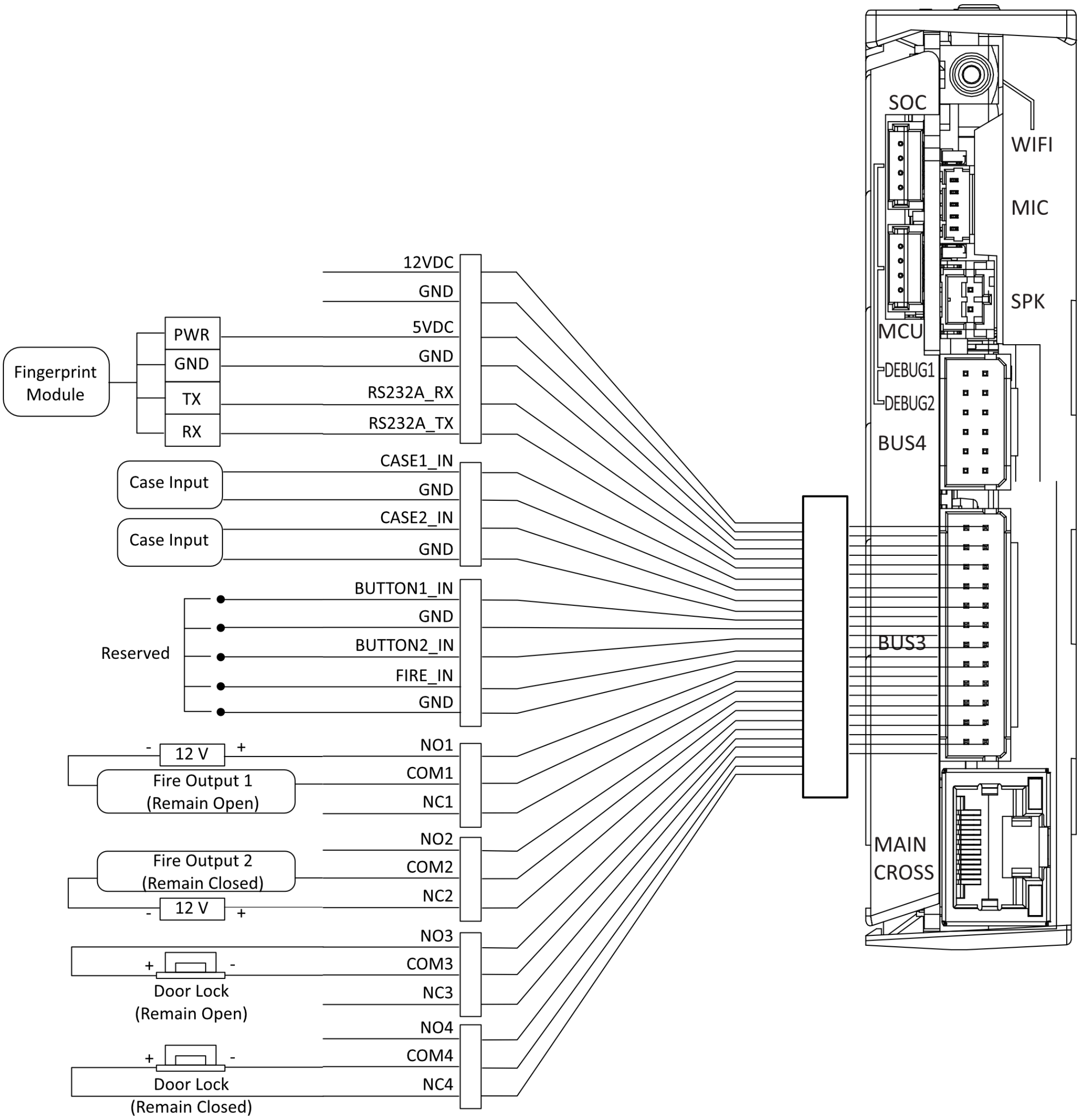


Figure 4-9 Wring Diagram of BUS3 Interface

Note

RS-232A corresponds to UART 1 on web.

4.5.4 Main Extended Interface Board Terminal Description

The main extended interface board contains the Wiegand/exit button interface and communication interface.

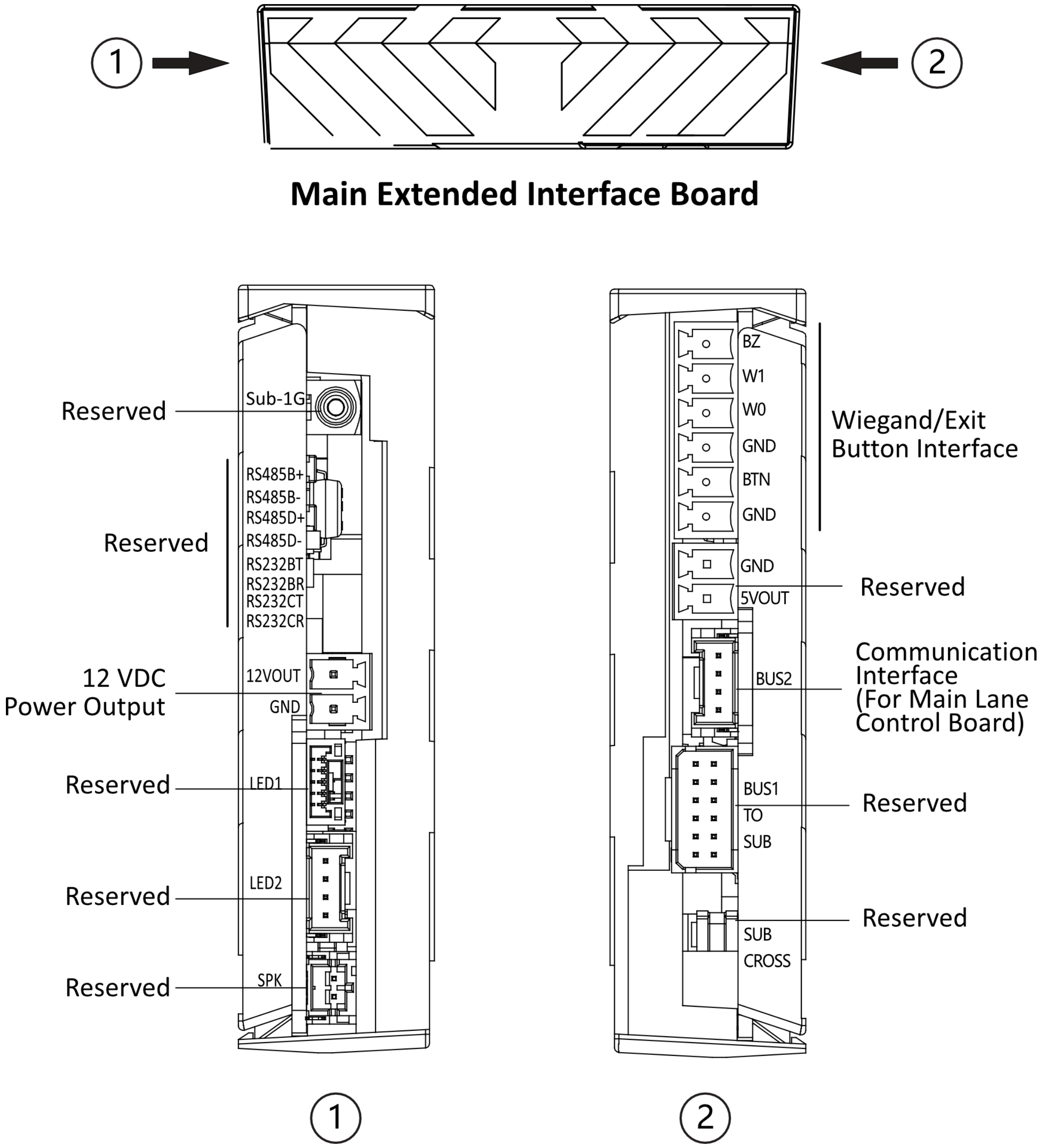


Figure 4-10 Main Optional Board Terminal

4.5.5 Sub Extended Interface Board Terminal Description

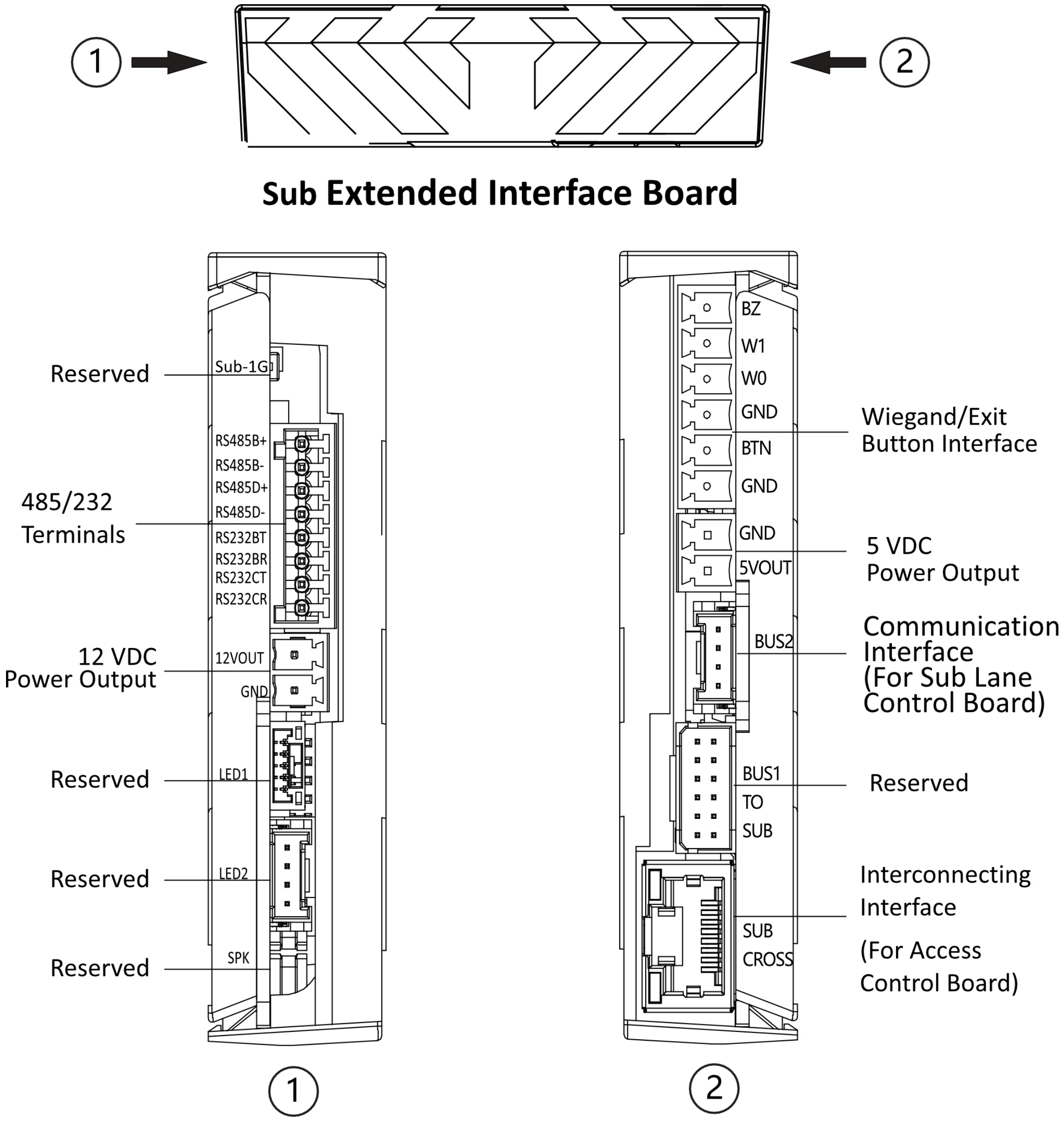


Figure 4-11 Sub Extended Interface Board

Note

- RS-485B corresponds to UART 6 on web and is for QR code scanner connection at exit by default.
- RS-485D corresponds to UART 4 on web and is for card reader connection at exit by default.
- RS-232B corresponds to UART 2 on web.
- RS-232C corresponds to UART 3 on web.

4.5.6 Card Reader Board Terminal Description

The card reader board can be connected to the access control board via RS-485 interface.

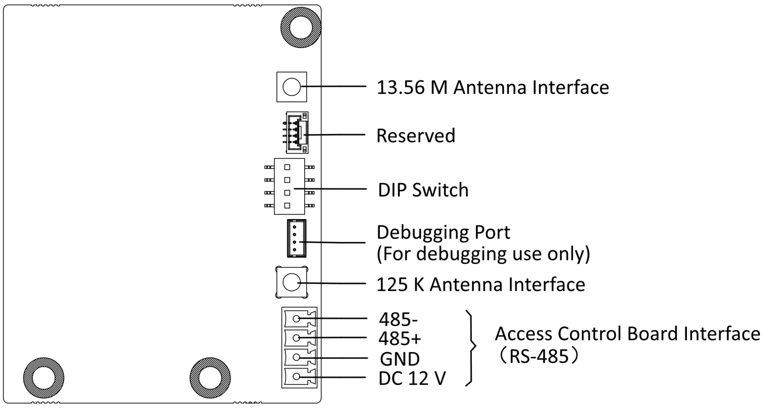


Figure 4-12 Card Reader Board

4.5.7 Lane Status Indicator Board

Appearance

Lane status indicator board is shown as follows.

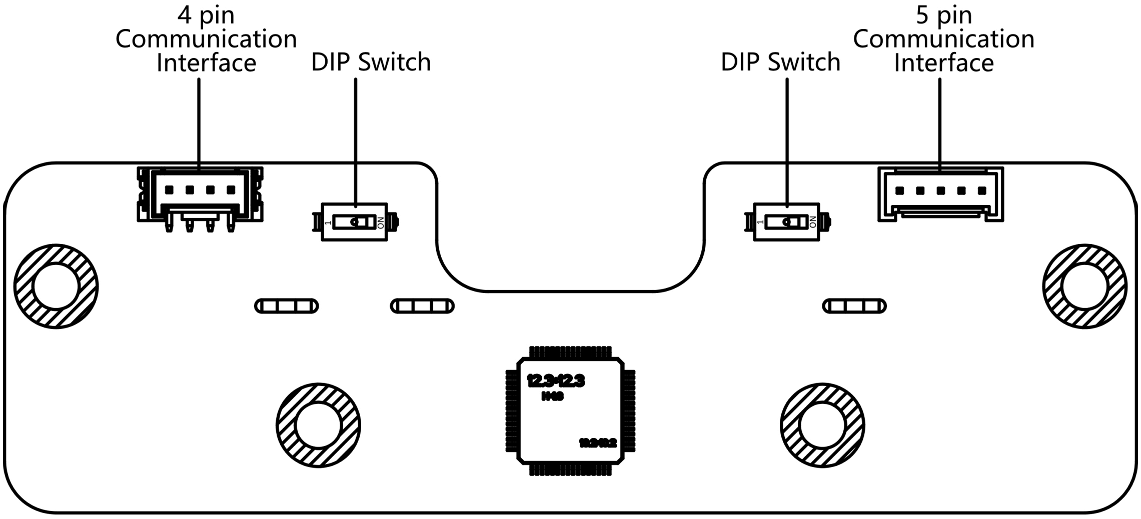


Figure 4-13 Lane Status Indicator Board

DIP Switch

Entrance

Set both DIP switches on the lane status indicator board at entrance to "ON" side:

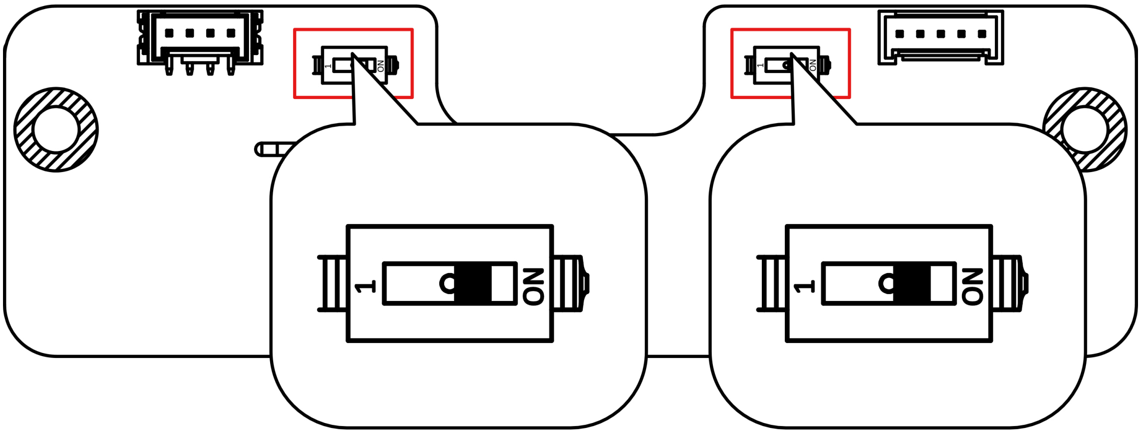


Figure 4-14 DIP Switch for Entrance

Entrance

Set both DIP switches on the lane status indicator board at exit to "1" side:

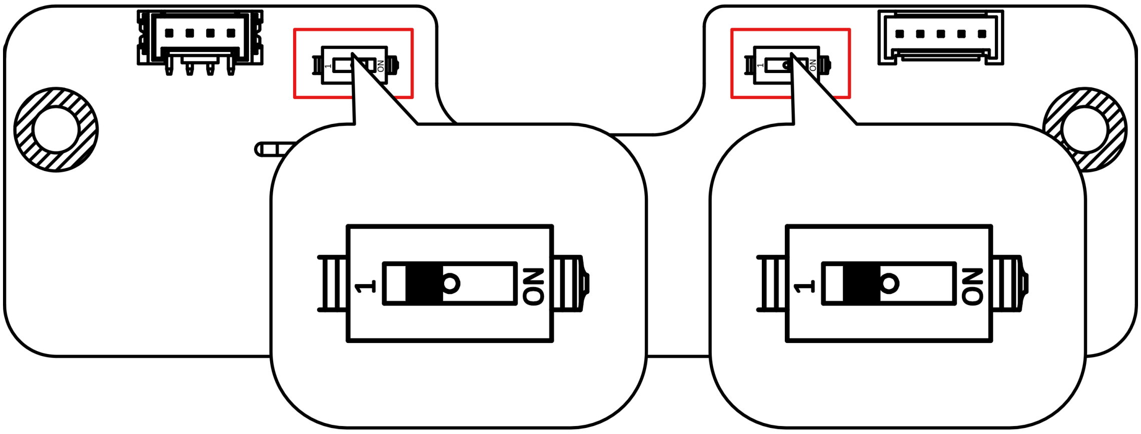


Figure 4-15 DIP Switch for Exit

Wiring

Lane status indicator board wiring diagram is shown as follows.

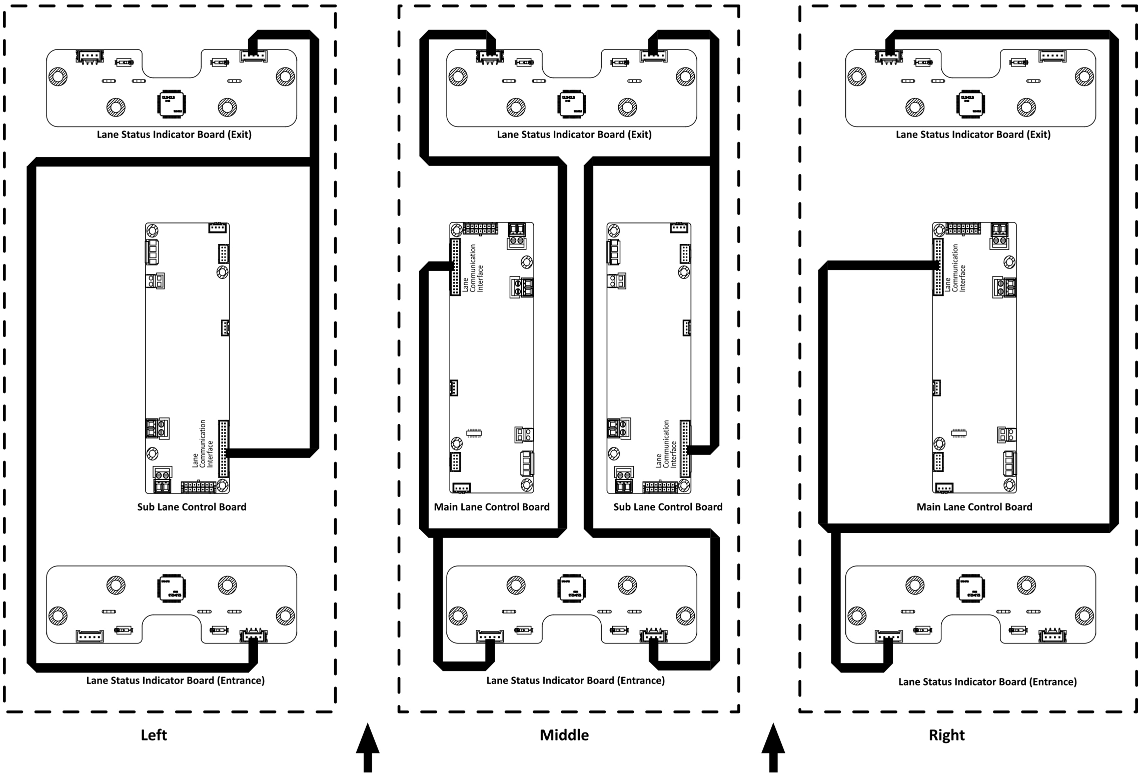

Lane Status Indicator Board (Exit)
Sub Lane Control Board
Lane Communication Interface
Lane Status Indicator Board (Entrance)
Lane Status Indicator Board (Exit)
Lane Communication Interface
Main Lane Control Board
Lane Communication Interface
Sub Lane Control Board
Lane Status Indicator Board (Entrance)
Lane Status Indicator Board (Exit)
Lane Communication Interface
Main Lane Control Board
Lane Status Indicator Board (Entrance)
Left
Middle
Right
Entrance

Figure 4-16 Lane Status Indicator Board Wiring

4.5.8 Wiring Diagram

The wiring diagram of components and peripherals.

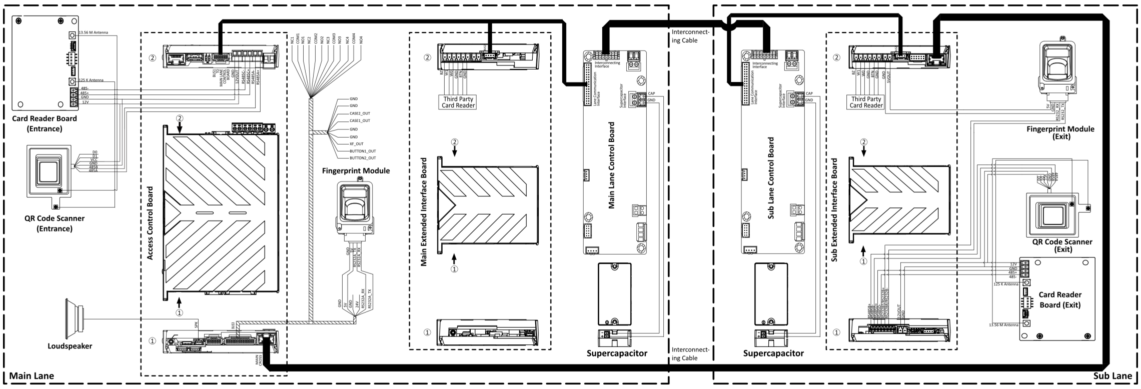


Figure 4-17 General Wiring

Note

- The supplied 2 interconnecting cables need connecting on-site:
  1. Communication cable for connection between main lane control board and sub lane control board. The cable is 5.5 m in length and put inside the package of the right/middle pedestal.
  2. CAT5e Communication cable. The cable is 5.5 m in length and put inside the package of the right/middle pedestal.
- The ① and ② refer to the two sides of a same board.
- Barrier opens at the entrance/exit: connect to BTN1/BTN2 and GND.

4.5.9 RS-485 Wiring

The RS-485 interfaces on the access control board and sub extended interface board are suggested to connect with the face recognition module or the card reader. Here takes connecting with a card reader as an example.

Note

- There are 2 RS-485 interfaces on the access control board for entrance. Refer to ***Access Control Board Terminal Description*** for details.
  There are 2 RS-485 interfaces on the sub extended interface board for exit. Refer to ***Sub Extended Interface Board Terminal Description*** for details.
- If connecting the RS-485 with a card reader, by default, the DIP switch of the card reader should be set as follows:
  - For entrance, set the No.1 of the 4-digit DIP switch to ON side.
  - For exit, set the No.3 of the 4-digit DIP switch to ON side.
- If there are other RS-485 devices connecting, the ID of the RS-485 cannot be conflicted.
- The connected 12 V power interface for the face recognition terminal cannot be connected with other 12 V devices.

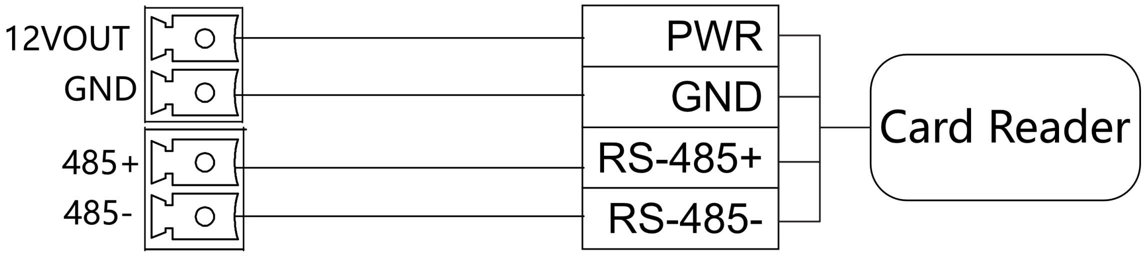


Figure 4-18 Wiring RS-485

4.5.10 Face Recognition Module Wiring

Connect the face recognition module to the turnstile.

The wiring diagram is shown as follows:

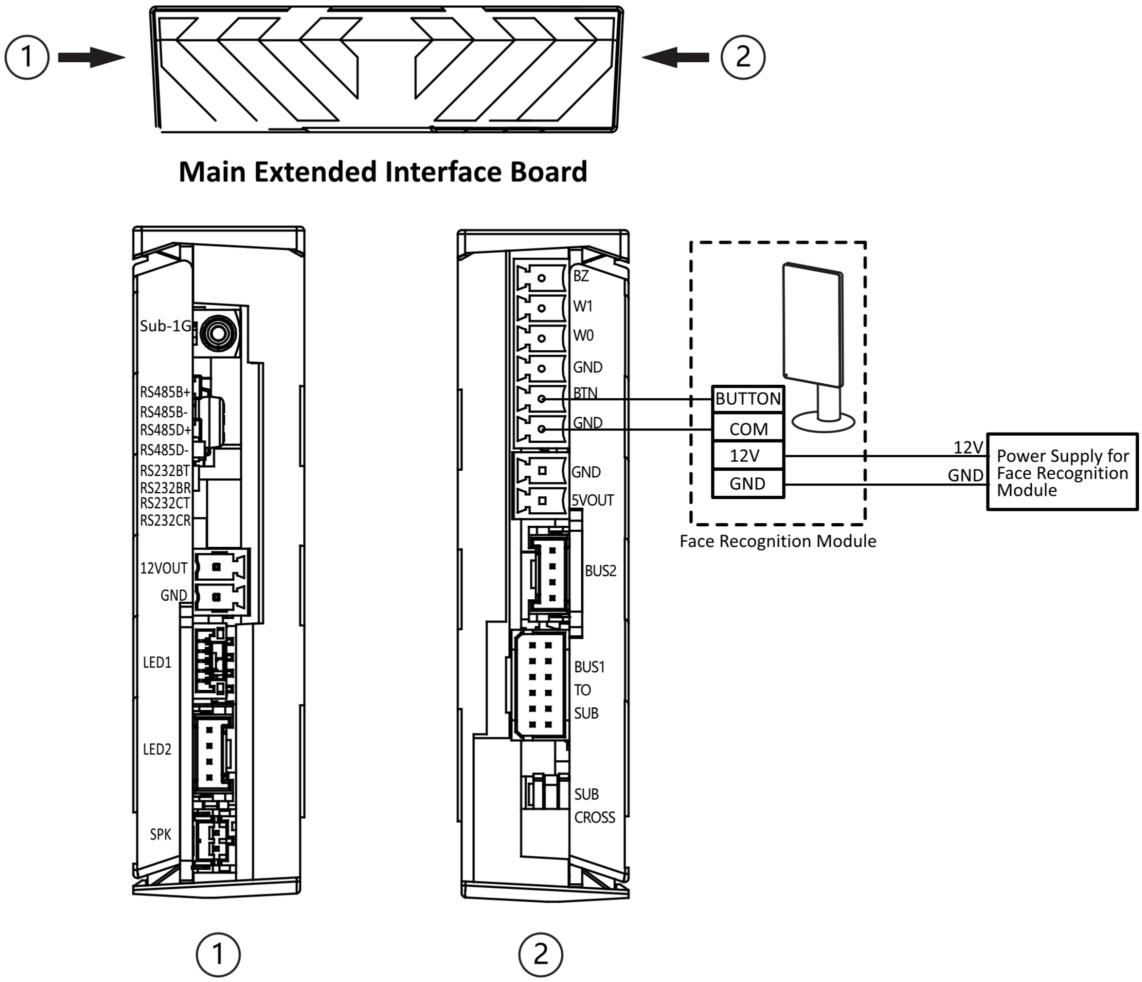


Figure 4-19 Face Recognition Module Wiring (Entrance)

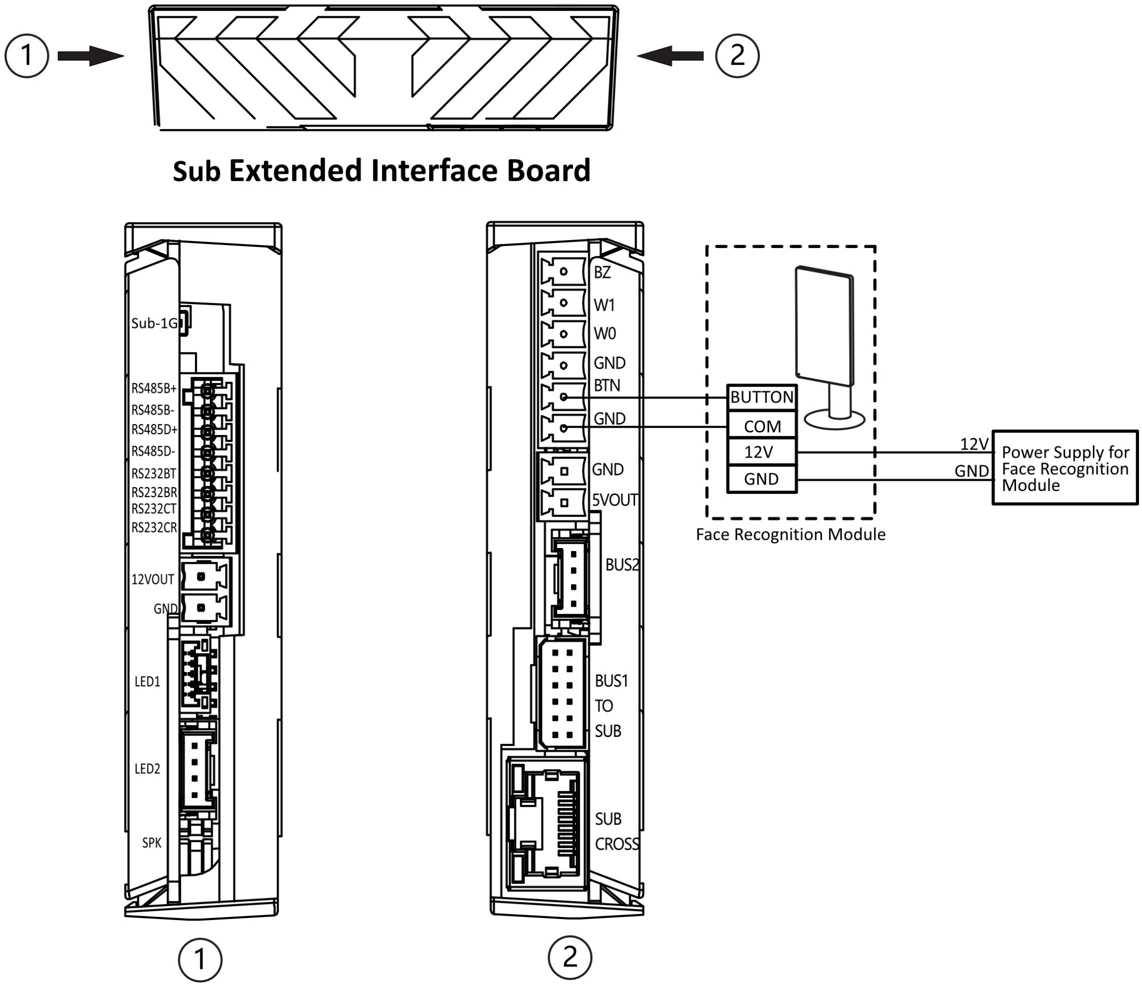


Figure 4-20 Face Recognition Module Wiring (Exit)

Chapter 5 Device Settings

After installation and wiring completed, you should set the barriers closed position (study mode) before entering the working mode.

You can also set the test mode, normal mode, passing mode and memory mode, pair the keyfob, or initialize the hardware by setting the DIP switch on the access control board.

- Study Mode: The barrier will learn the closed position.
- Normal Mode: The device will work properly.
- Test Mode: Test mode is the same as the normal mode except that the device cannot report the alarm, the event, or the people counting information to the center.
- Memory Mode: By default, the memory mode is enabled. When multiple cards are presented and authenticated, it allows multiple persons passing through the lane. When it counts the passing people number is equal to the card presented times, or no person passing through the lane after the last person passing, the barriers will be closed.

5.1 Set Study Mode

Enter the study mode through DIP switching to set the closed position of the device barrier.

Steps

1. Set the No.1 of the 2-digit DIP switch on the access control board to ON by referring the following figure to enter the study mode.

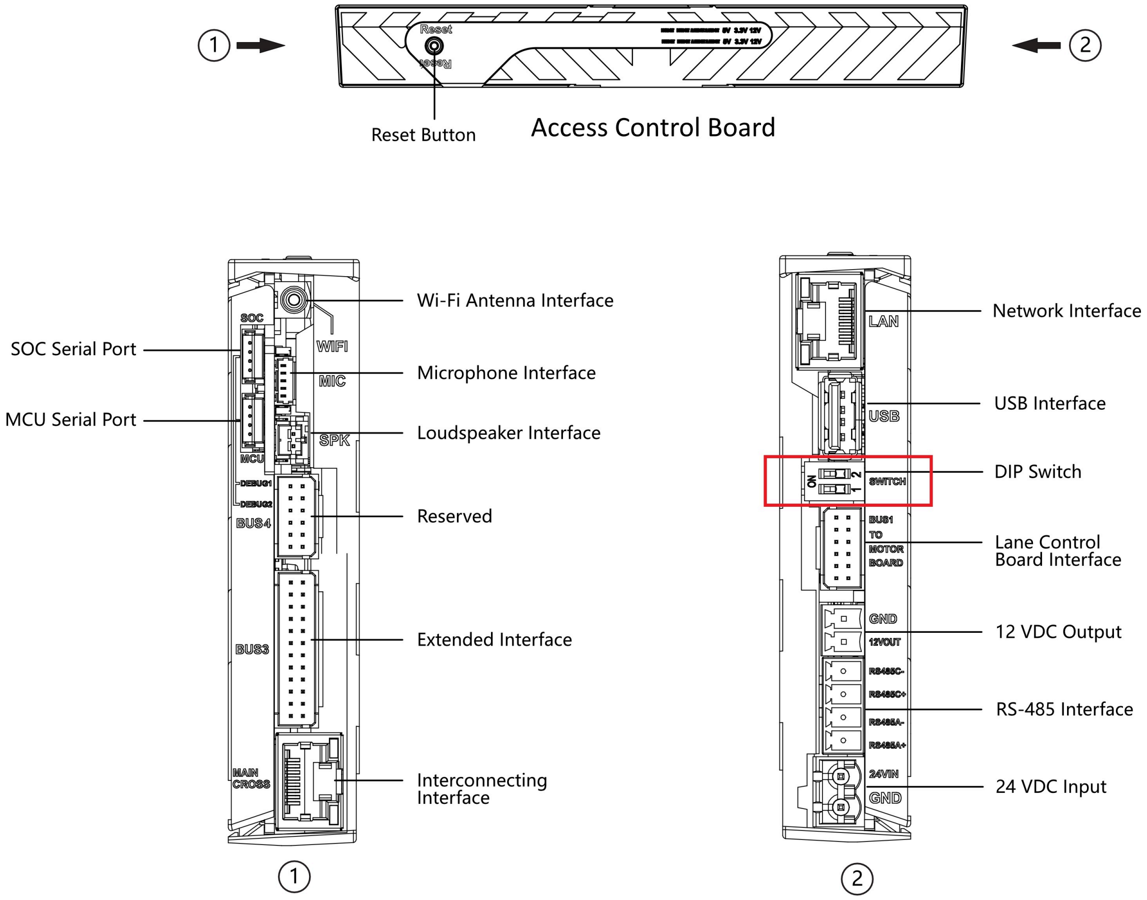


Figure 5-1 DIP Switch Location

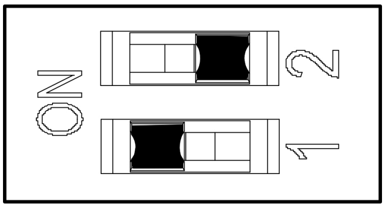


Figure 5-2 Study Mode

2. Adjust the closed position of the barrier.
3. Power on the device.

   The device will remember the current position (closed position) automatically.
4. Power off the device.
5. Set the No.1 switches of the 2-digit DIP Switch on the main user extended interface board by referring to the following figure.

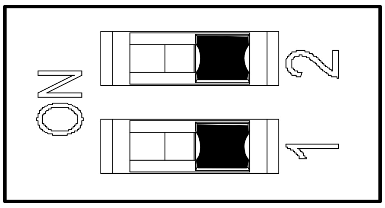


Figure 5-3 Normal Mode

6. Power on the device again.

Note

For details about the DIP switch value and meaning, see *DIP Switch Description*.

The barrier will open automatically and turns back to the closed position. At this circumstance, the device enters the normal mode.

5.2 Pair Keyfob

Pair the remote control to the device through DIP switch to open/close the barrier remotely.

Before You Start

Ask our technique supports or sales and purchase the keyfob.

Steps

1. Power off the turnstile.
2. Set the No.2 switch of the DIP Switch on the access control board to the ON side.

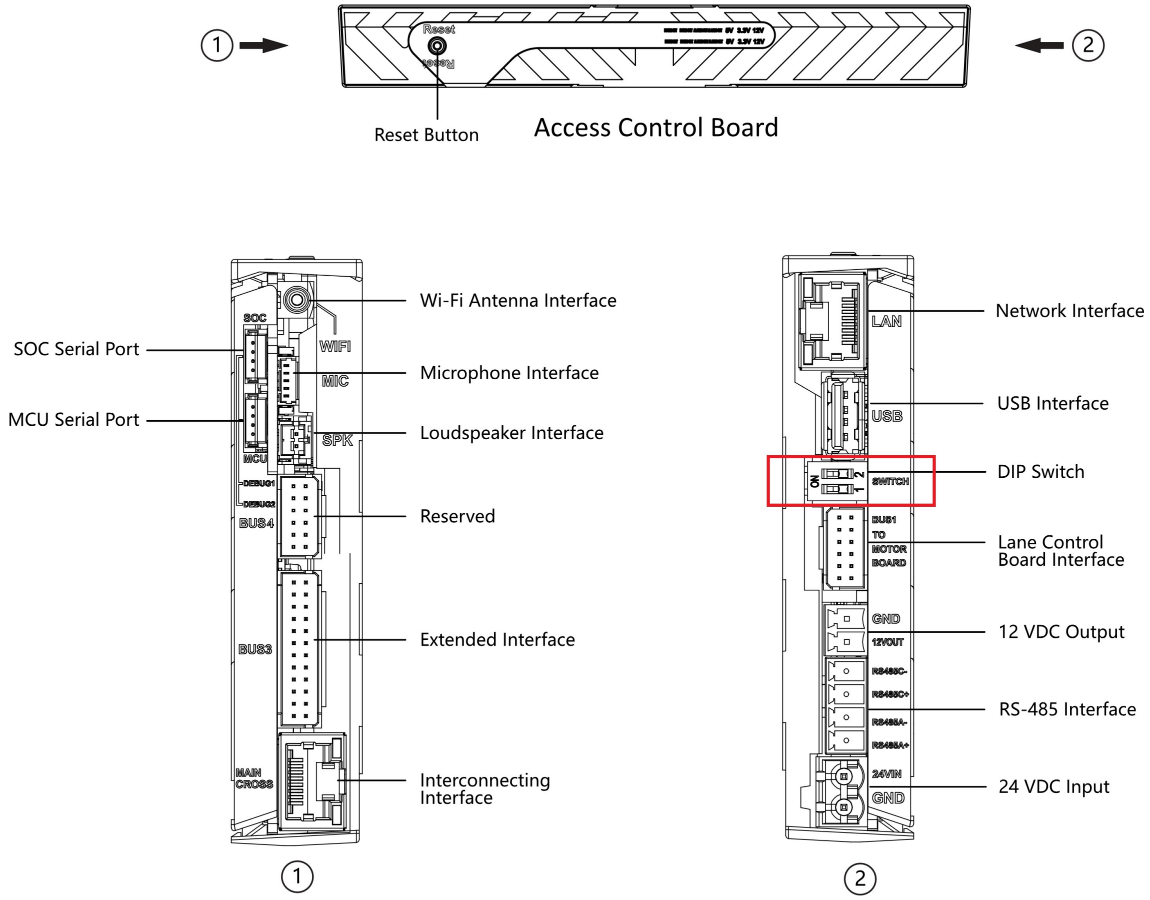


Figure 5-4 DIP Switch Location

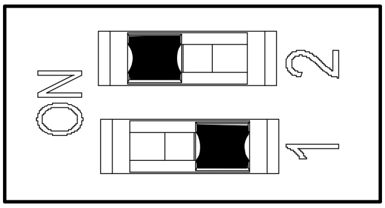


Figure 5-5 Enable Keyfob Paring Mode

3. Power on the turnstile and it will enter the keyfob pairing mode.
4. Hold the **Close** button for more than 10 seconds.

   The keyfob's indicator of the will flash twice if the pairing is completed.
5. Set the No.2 switch to the OFF side, and reboot the turnstile to take effect.

Note

- Only one turnstile can pair the keyfob. If multiple turnstiles are in the pairing mode, the keyfob will select only one of them to pair.
- For details about DIP switch value and meaning, see ***DIP Switch Description*** .

6. **Optional:** Go to **System → User → Keyfob User** on the remote control page of the client software to delete the keyfob.

5.3 Initialize Device

Steps

1. Hold the initialization button on the access control board for 5 s.

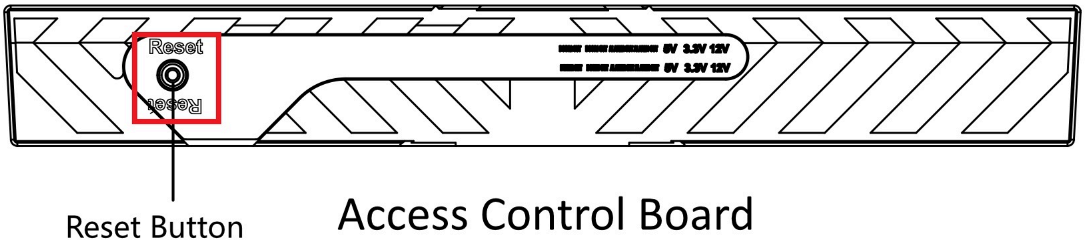


Figure 5-6 Initialization Button Position

2. The device will start restoring to factory settings.
3. When the process is finished, the device will beep for 3 s.

Caution

The initialization of the device will restore all the parameters to the default setting and all the device events are deleted.

Note

Make sure no persons are in the lane when powering on the device.

Chapter 6 Activation

You should activate the device before the first login. After powering on the device, the system will switch to Device Activation page.

Activation via the device, SADP tool and the client software are supported.

The default values of the device are as follows:

- The default IP address: 192.0.0.64
- The default port No.: 8000
- The default user name: admin

6.1 Activate via SADP

SADP is a tool to detect, activate and modify the IP address of the device over the LAN.

Before You Start

- Get the SADP software from the supplied disk or the official website ***http://www.hikvision.com/en/*** , and install the SADP according to the prompts.
- The device and the PC that runs the SADP tool should be within the same subnet.

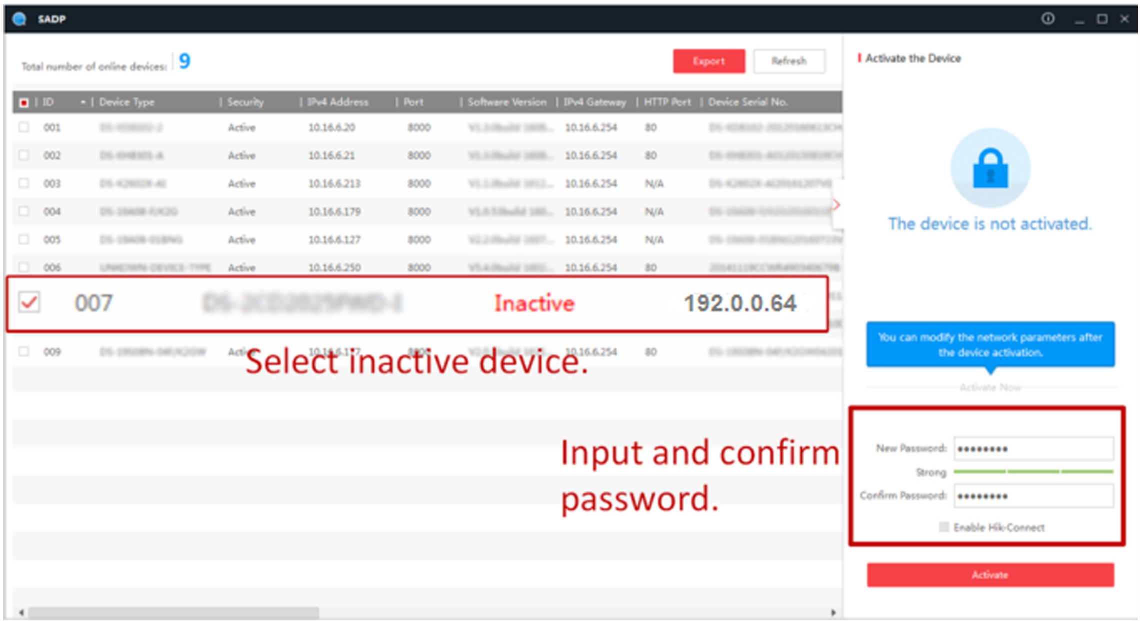
The following steps show how to activate a device and modify its IP address. For batch activation and IP addresses modification, refer to *User Manual of SADP* for details.

Steps

1. Run the SADP software and search the online devices.
2. Find and select your device in online device list.
3. Input new password (admin password) and confirm the password.

   ⚠ **Caution**

   STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.
4. Click **Activate** to start activation.



SADP

Total number of online devices: 9

ID	Device Type	Security	IPv4 Address	Port	Software Version	IPv4 Gateway	HTTP Port	Device Serial No.
☐ 001	[illegible]	Active	10.16.6.20	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 002	[illegible]	Active	10.16.6.21	8000	[illegible]	10.16.6.254	80	[illegible]
☐ 003	[illegible]	Active	10.16.6.213	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 004	[illegible]	Active	10.16.6.179	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 005	[illegible]	Active	10.16.6.127	8000	[illegible]	10.16.6.254	N/A	[illegible]
☐ 006	[illegible]	Active	10.16.6.250	8000	[illegible]	10.16.6.254	80	[illegible]
☑ 007	[illegible]	Inactive	192.0.0.64					
☐ 009	[illegible]	Active	[illegible]	[illegible]	[illegible]	10.16.6.254	80	[illegible]

Select inactive device.

Activate the Device

The device is not activated.

You can modify the network parameters after the device activation.

New Password: ••••••••

Strong

Confirm Password: ••••••••

☐ Enable Hik-Connect

Input and confirm password.

Status of the device becomes **Active** after successful activation.

5. Modify IP address of the device.
   1) Select the device.
   2) Change the device IP address to the same subnet as your computer by either modifying the IP address manually or checking **Enable DHCP**.
   3) Input the admin password and click **Modify** to activate your IP address modification.

6.2 Activate Device via Client Software

For some devices, you are required to create the password to activate them before they can be added to the software and work properly.

Steps

Note

This function should be supported by the device.

1. Enter the Device Management page.
2. Click ▴ on the right of **Device Management** and select **Device**.
3. Click **Online Device** to show the online device area.

   The searched online devices are displayed in the list.
4. Check the device status (shown on **Security Level** column) and select an inactive device.
5. Click **Activate** to open the Activation dialog.
6. Create a password in the password field, and confirm the password.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7. Click **OK** to activate the device.

6.3 Activate via Web Browser

You can activate the device via the web browser.

Steps

1. Enter the device default IP address (192.0.0.64) in the address bar of the web browser, and press **Enter**.

Note

Make sure the device IP address and the computer's should be in the same IP segment.

2. Create a new password (admin password) and confirm the password.

Caution

STRONG PASSWORD RECOMMENDED-We highly recommend you create a strong password of your own choosing (using a minimum of 8 characters, including upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you reset your password regularly, especially in the high security system, resetting the password monthly or weekly can better protect your product.

3. Click **Activate**.
4. Edit the device IP address. You can edit the IP address via the SADP tool, the device, and the client software.

Chapter 7 Operation via Web Browser

7.1 Login

You can login via the web browser or the remote configuration of the client software.

Note

Make sure the device is activated.

Login via Web Browser

Enter the device IP address in the address bar of the web browser and press **Enter** to enter the login page.
Enter the device user name and the password. Click **Login**.

Login via Remote Configuration of Client Software

Download and open the client software. After adding the device, click ⚙ to enter the Configuration page.

7.2 Web Wizard

7.2.1 Time Settings

Click ➤ in the top right of the web page to enter the wizard page.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address/NTP Port/Interval

You can set the server address, NTP port, and interval.

DST

You can view the DST start time, end time and bias time.

Click **Next** to save the settings and go to the next parameter. Or click **Skip** to skip time settings.

7.2.2 Administrator Settings

Steps

1. Click ◁ in the top right of the web page to enter the wizard page. After time settings, you can click **Next** to enter the **Administrator Settings** page.
2. Enter the employee ID and name of the administrator.
3. Add card.

   1) Click**+** to add card.

   Note

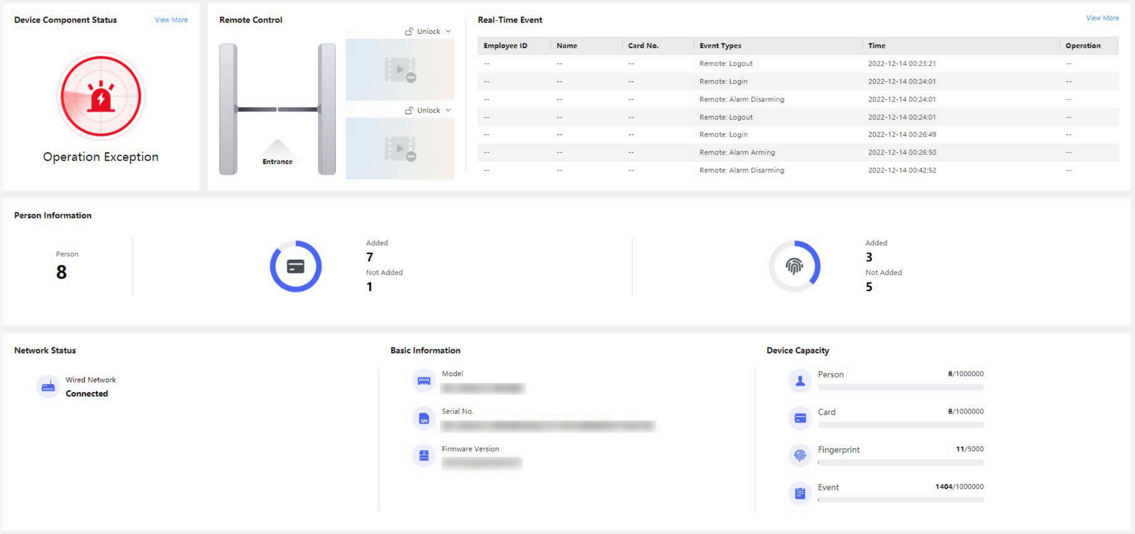
   Up to 5 cards can be supported.

   2) enter the Card No. and select the property of the card.

   Click **Complete** to complete the settings.

7.3 Overview

You can view the device component status, real-time event, person information, network status, basic information, and device capacity. You can also control the barrier remotely.



Employee ID	Name	Card No.	Event Types	Time	Operation
--	--	--	Remote: Logout	2022-12-14 00:23:21	--
--	--	--	Remote: Login	2022-12-14 00:24:01	--
--	--	--	Remote: Alarm Disarming	2022-12-14 00:24:01	--
--	--	--	Remote: Logout	2022-12-14 00:24:01	--
--	--	--	Remote: Login	2022-12-14 00:26:49	--
--	--	--	Remote: Alarm Arming	2022-12-14 00:26:50	--
--	--	--	Remote: Alarm Disarming	2022-12-14 00:42:52	--

Person Information

Person 8

Added 7
Not Added 1

Added 3
Not Added 5

Network Status

Wired Network
Connected

Basic Information

Model
[redacted]

Serial No.
[redacted]

Firmware Version
[redacted]

Device Capacity

Person	8/1000000
Card	8/1000000
Fingerprint	11/5000
Event	1404/1000000

Figure 7-1 Overview

Function Descriptions:

Device Component Status

You can check if the device is working properly. Click **View More** to view the detailed component status.

Remote Control

🔓 / 🔒 / ▣ / ▣

The door is opened/closed/remaining open/remaining closed.

Real-Time Event

You can view the event Employee ID, Name, Card No., Event Type, Time, and Operation. You can also click **View More** to enter the event search page.

Person Information

You can view the quantity information of person, card and fingerprint.

Network Status

You can view the network connection status.

Basic Information

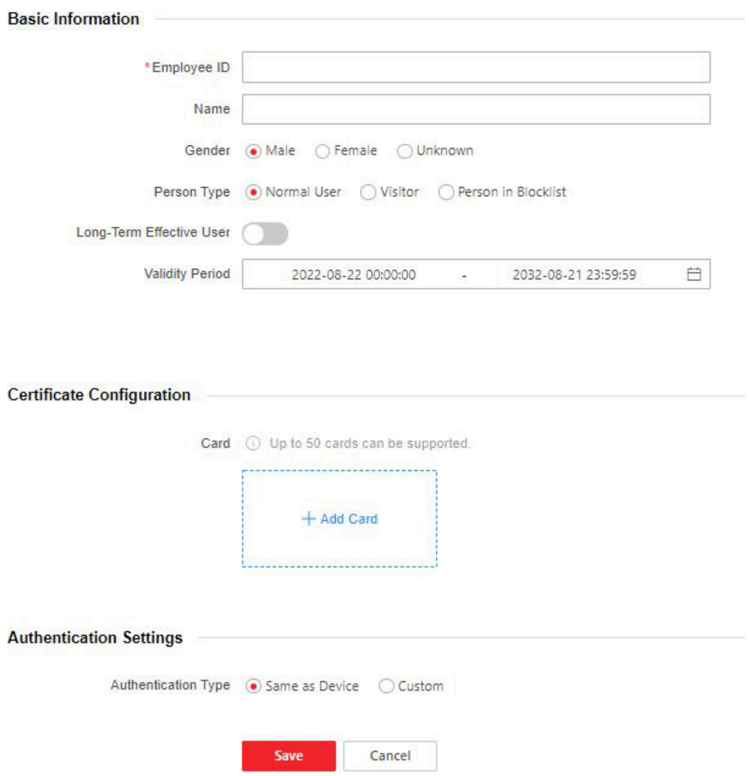
You can view the model, serial No. and firmware version.

Device Capacity

You can view the person, card, fingerprint and event capacity.

7.4 Person Management

Click **Add** to add the person's information, including the basic information, certificate, authentication and settings.



Basic Information

*Employee ID

Name

Gender ● Male ○ Female ○ Unknown

Person Type ● Normal User ○ Visitor ○ Person in Blocklist

Long-Term Effective User

Validity Period 2022-08-22 00:00:00 - 2032-08-21 23:59:59

Certificate Configuration

Card ⓘ Up to 50 cards can be supported.

Authentication Settings

Authentication Type ● Same as Device ○ Custom

Figure 7-2 Add Person

Add Basic Information

Click **Person Management → Add** to enter the Add Person page.

Add the person's basic information, including the employee ID, the person's name, person type,etc.

If you select **Visitor** as the person type, you can set the visit times.

Click **Save** to save the settings.

Set Permission Time

Click **Person Management → Add** to enter the Add Person page.

Enable **Long-Term Effective User**, or set **Validity Period** and the person can only has the permission within the configured time period according to your actual needs.

Click **Save** to save the settings.

Add Card

Click **Person Management → Add** to enter the Add Person page.

Click **Add Card**, enter the **Card No.** and select the **Property**, and click **OK** to add the card.

Note

Up to 50 cards can be added.

Click **Save** to save the settings.

Authentication Settings

Click **Person Management → Add** to enter the Add Person page.
Set **Authentication Type** as **Same as Device** or **Custom**.
Click **Save** to save the settings.

Import/Export Person Data

Export Person Data

You can export added person data for back-up or importing to other devices.

Click **Export Person Data**, set an encryption password and confirm it. Click **OK**.

Note

- The person data will be downloaded to your PC.
- The password you set will be required for importing the data file.

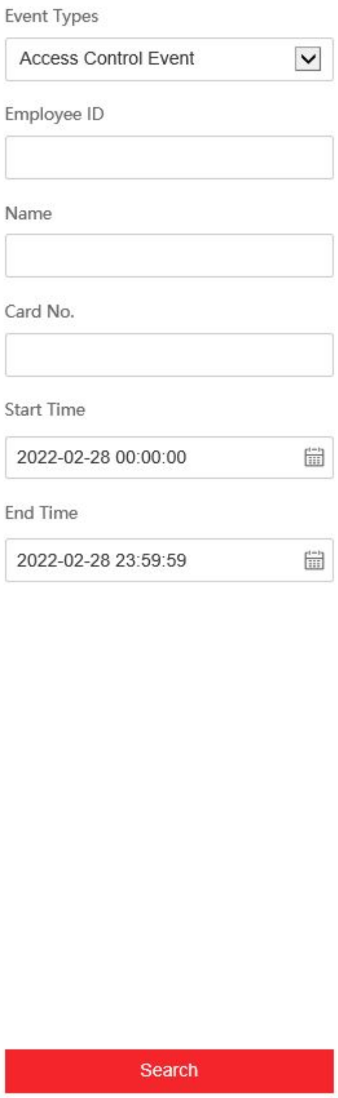
Importing Person Data

Click **Importing Person Data** and select the file. Click **Import**.

Enter the encryption password to import and synchronize the person data to devices.

7.5 Search Event

Click **Event Search** to enter the Search page.



Event Types

Access Control Event

Employee ID

Name

Card No.

Start Time

2022-02-28 00:00:00

End Time

2022-02-28 23:59:59

Figure 7-3 Search Event

Select the event type and enter the search conditions, including the employee ID, name, card No., start time, and end time, and click **Search**.

The results will be displayed on the right panel.

7.6 Configuration

7.6.1 View Device Information

Click **Configuration → System → System Settings → Basic Information** to enter the configuration page.

You can view the device name, language, model, serial No., version, IO input, IO output, and local RS-485 number.

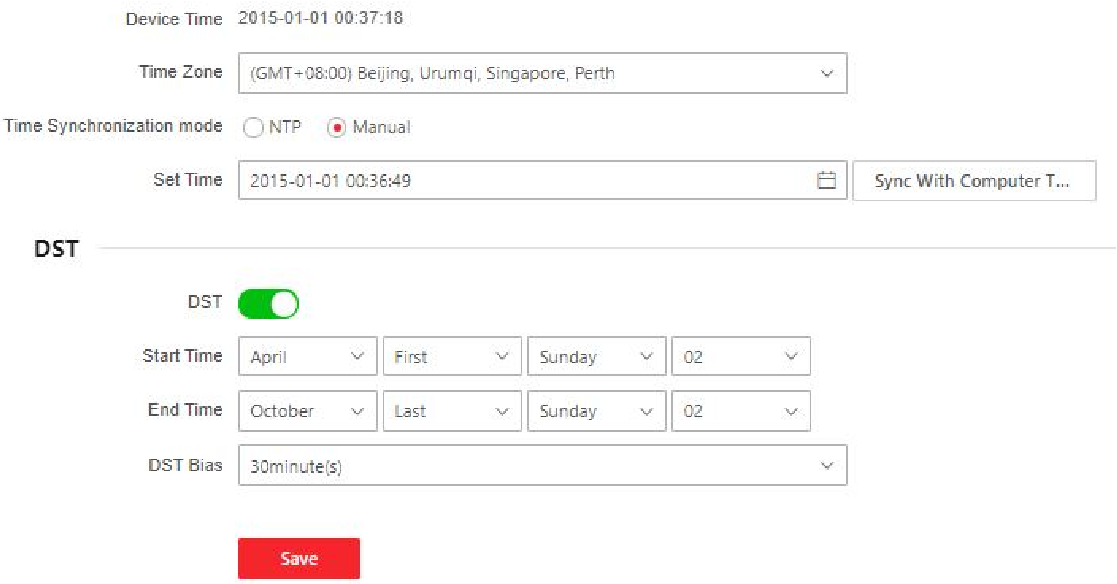
You can change **Device Name** and click **Save**.

You can view the device capacity, including person, card, fingerprint and event.

7.6.2 Set Time

Set the device's time.

Click **Configuration → System → System Settings → Time Settings** .



Device Time 2015-01-01 00:37:18

Time Zone (GMT+08:00) Beijing, Urumqi, Singapore, Perth

Time Synchronization mode ○ NTP ● Manual

Set Time 2015-01-01 00:36:49 Sync With Computer T...

DST

DST

Start Time April First Sunday 02

End Time October Last Sunday 02

DST Bias 30minute(s)

Figure 7-4 Time Settings

Click **Save** to save the settings after the configuration.

Time Zone

Select the device located time zone from the drop-down list.

Time Sync.

NTP

You should set the NTP server's IP address, port No., and interval.

Manual

By default, the device time should be synchronized manually. You can set the device time manually or check **Sync. with Computer Time** to synchronize the device time with the computer's time.

Server Address Type/Server Address/NTP Port/Interval

You can set the server address type, server address, NTP port, and interval.

7.6.3 Set DST

Steps

1. Click **Configuration → System → System Settings → Time Settings** .
2. Enable **DST**.
3. Set the DST start time, end time and bias time.
4. Click **Save** to save the settings.

7.6.4 Change Administrator's Password

Steps

1. Click **Configuration → System → User Management** .
2. Click ✎ .
3. Enter the old password and create a new password.
4. Confirm the new password.
5. Click **Save**.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

7.6.5 Online Users

The information of users logging into the device is shown.

Go to **Configuration → User Management → Online Users** to view the list of online users.

7.6.6 View Device Arming/Disarming Information

View device arming type and arming IP address.

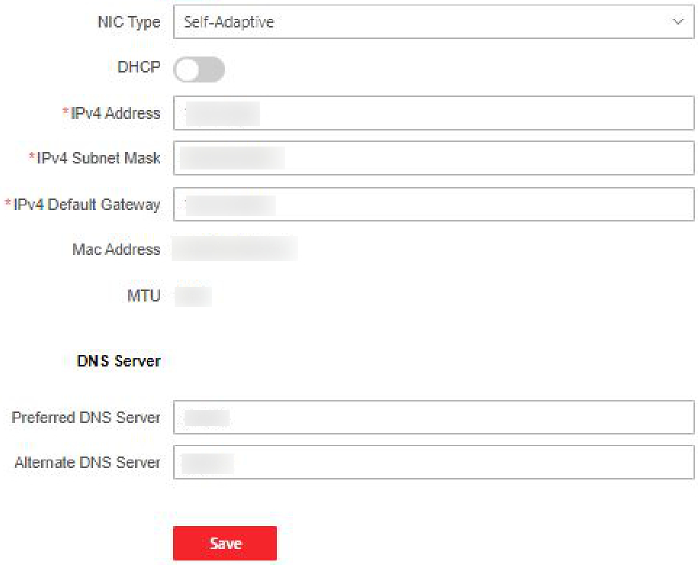
Go to **Configuration → User Management → Arming/Disarming Information** .
You can view the device arming/disarming information. Click **Refresh** to refresh the page.

7.6.7 Network Settings

Set TCP/IP and port.

Set Basic Network Parameters

Click **Configuration → Network → Network Settings → TCP/IP** .



NIC Type: Self-Adaptive

DHCP

*IPv4 Address

*IPv4 Subnet Mask

*IPv4 Default Gateway

Mac Address

MTU

DNS Server

Preferred DNS Server

Alternate DNS Server

Figure 7-5 TCP/IP Settings Page

Set the parameters and click **Save** to save the settings.

NIC Type

Select a NIC type from the drop-down list. By default, it is **Self-Adaptive**.

DHCP

If you disable DHCP, you should manually set the IPv4 address, IPv4 subnet mask, IPv4 default gateway, preferred DNS server, and alternate DNS server.

If you enable DHCP, the system will automatically allocate the IPv4 address, IPv4 subnet mask, the IPv4 default gateway preferred DNS server and alternate DNS server.

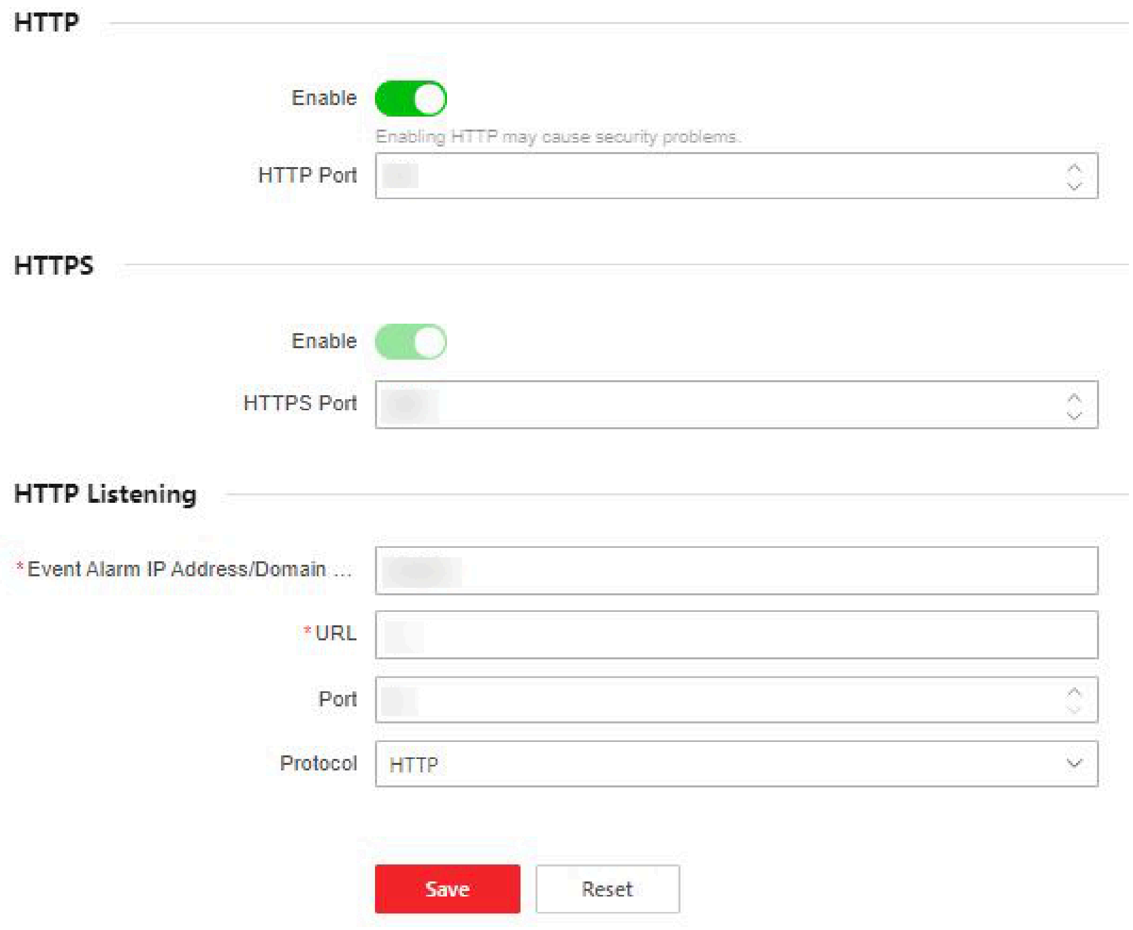
DNS Server

Set the preferred DNS server and the Alternate DNS server according to your actual need.

Set Port Parameters

Set the HTTP, HTTPS, and HTTP Listening parameters.

Click **Configuration → Network → Network Service → HTTP(S)** .



HTTP

Enable: on

Enabling HTTP may cause security problems.

HTTP Port

HTTPS

Enable: on

HTTPS Port

HTTP Listening

*Event Alarm IP Address/Domain ...

*URL

Port

Protocol: HTTP

Figure 7-6 Network Service

HTTP

It refers to the port through which the browser accesses the device. For example, when the HTTP Port is modified to 81, you need to enter ***http://192.0.0.65:81*** in the browser for login.

HTTPS

Set the HTTPS for accessing the browser. Certificate is required when accessing.

HTTP Listening

The device can send alarm information to the event alarm IP address or domain name via HTTP protocol/HTTPS protocol. Edit the event alarm IP address or domain name, URL, port, and protocol.

Note

The event alarm IP address or domain name should support the HTTP protocol/HTTPS protocol to receive the alarm information.

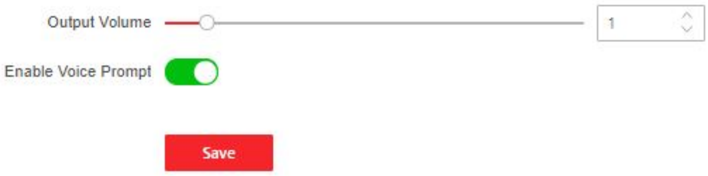
.

7.6.8 Set Audio Parameters

Set the image quality, resolution, and the device volume.

Set Audio Parameters

Click **Configuration → Video/Audio → Audio** .



Output Volume: 1

Enable Voice Prompt: ●

Figure 7-7 Set Audio Parameters

Drag the block to adjust the output volume.
Click **Save** to save the settings after the configuration.
You can also enable **Voice Prompt**.

Note

The functions vary according to different models. Refers to the actual device for details.

7.6.9 Event Linkage

Set linked actions for events.

Steps

1. Click **Configuration → Event → Event Detection → Linkage Settings** to enter the page.
2. Set event source.
   - If you choose **Linkage Type** as **Event Linkage**, you need to select event types from the drop-down list.

- If you choose **Linkage Type** as **Card Linkage**, you need to enter the card No. and select the card reader.
- If you choose **Linkage Type** as **Employee ID Linkage**, you need to enter the employee ID and select the card reader.

3. Set linked action.

Linked Buzzer

Enable **Linked Buzzer** and select **Start Buzzing** or **Stop Buzzing** for the target event.

Linked Door

Enable **Linked Door**, check **Entrance** or **Exit**, and set the door status for the target event.

Linked Alarm Output

Enable **Linked Alarm Output**, check **Alarm Output 1** or **Alarm Output 2**, and set the alarm output status for the target event.

Linked Audio Prompt

Enable **Linked Audio Prompt** and select the play mode.

- If you choose **TTS**, you need to set language and enter the prompt content.
- If you choose **Audio File**, you need to select an available audio file from the drop-down list or click **General Linkage Settings** to add a new audio file.

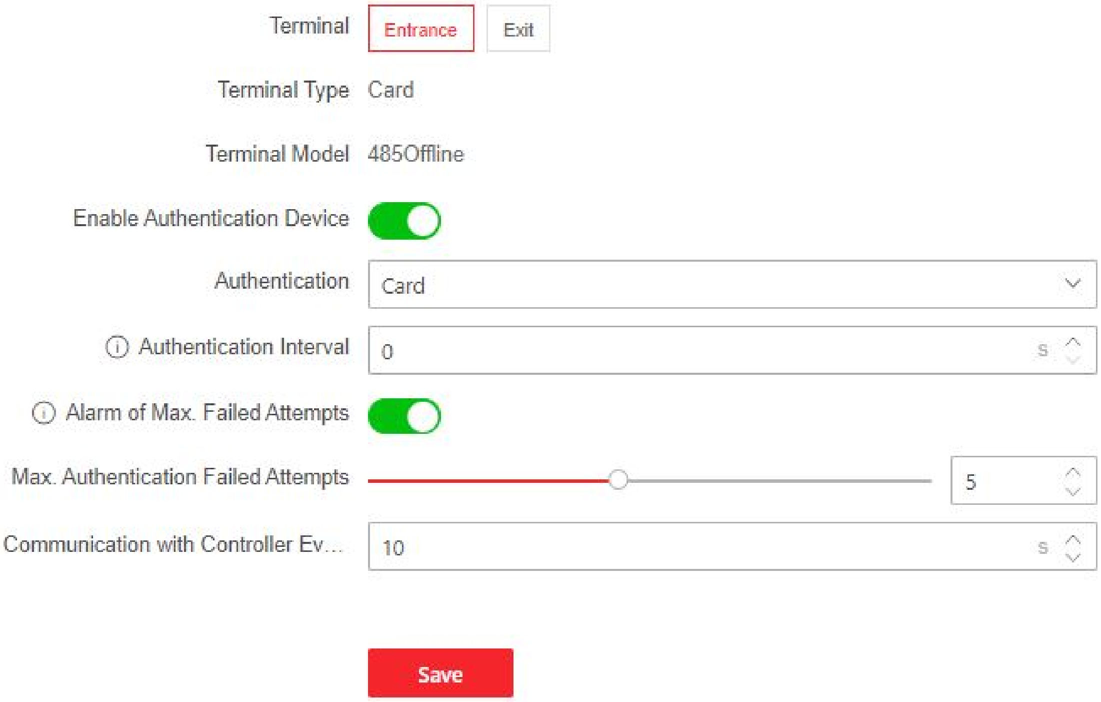
7.6.10 Access Control Settings

Set Authentication Parameters

Click **Configuration → Access Control → Authentication Settings** .

Note

The functions vary according to different models. Refers to the actual device for details.



Terminal: Entrance | Exit

Terminal Type: Card

Terminal Model: 485Offline

Enable Authentication Device: ●

Authentication: Card

Authentication Interval: 0 s

Alarm of Max. Failed Attempts: ●

Max. Authentication Failed Attempts: 5

Communication with Controller Ev...: 10 s

Figure 7-8 Set Authentication Parameters

Click **Save** to save the settings after the configuration.

Terminal

Choose **Entrance** or **Exit** for settings.

Terminal Type/Terminal Model

Get terminal description. They are read-only.

Enable Authentication Device

Enable the authentication function.

Authentication

Select an authentication mode according to your actual needs from the drop-down list.

Authentication Interval

You can set the authentication interval of the same person when authenticating. The same person can only authenticate once in the configured interval. A second authentication will be failed.

Alarm of Max. Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Max. Authentication Failed Attempts

Enable to report alarm when the card reading attempts reach the set value.

Communication with Controller Every

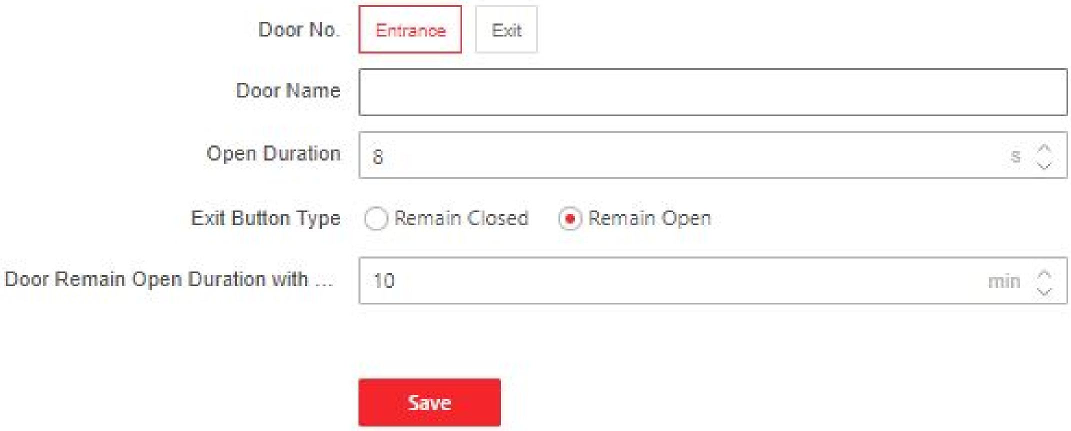
When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Note

The authentication interval value ranges from 2 s to 255 s.

Set Door Parameters

Click **Configuration → Access Control → Door Parameters** .



Door No. [✓ Entrance] Exit

Door Name

Open Duration 8 s

Exit Button Type ○ Remain Closed ● Remain Open

Door Remain Open Duration with ... 10 min

Figure 7-9 Door Parameters Settings Page

Click **Save** to save the settings after the configuration.

Door No.

Select **Entrance** or **Exit** for settings.

Door Name

You can create a name for the door.

Open Duration

Set the door unlocking duration. If the door is not opened for the set time, the door will be locked.

Note

The open duration ranges from 5 s to 60 s.

Exit Button Type

You can set the exit button as **Remain Open** or **Remain Closed** according to your actual needs. By default, it is **Remain Open**.

Door Remain Open Duration with First Person

Set the door open duration when first person is in. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Note

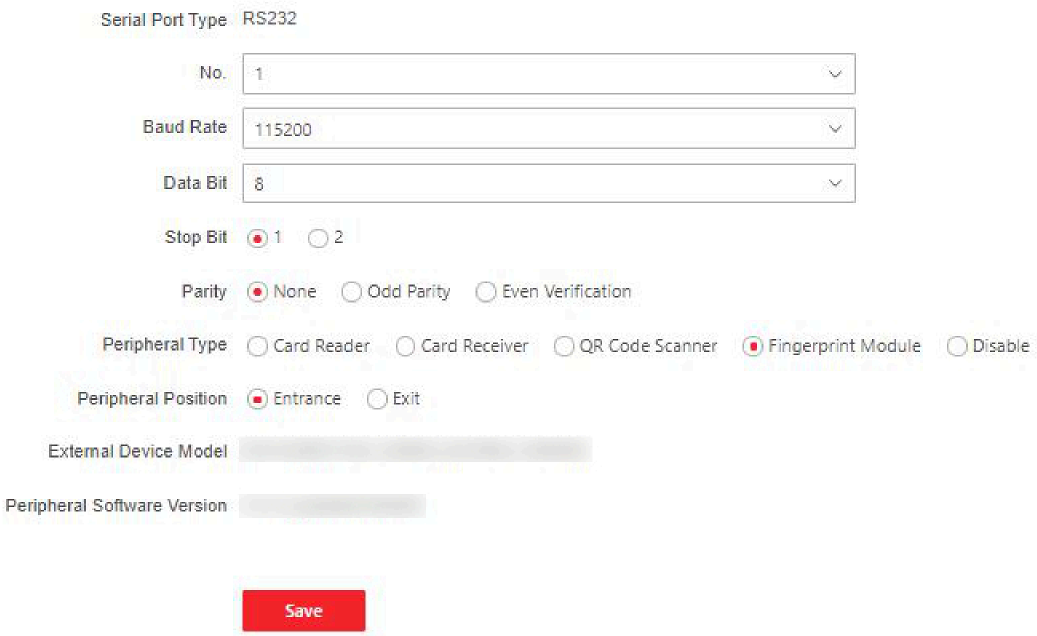
The duration ranges from 1 s to 1440 s.

Serial Port Settings

Set serial port parameters.

Steps

1. Click **Configuration → Access Control → Serial Port Configuration** .



Serial Port Type RS232

No. 1

Baud Rate 115200

Data Bit 8

Stop Bit ● 1 ○ 2

Parity ● None ○ Odd Parity ○ Even Verification

Peripheral Type ○ Card Reader ○ Card Receiver ○ QR Code Scanner ● Fingerprint Module ○ Disable

Peripheral Position ● Entrance ○ Exit

External Device Model [redacted]

Peripheral Software Version [redacted]

Figure 7-10 Serial Port Settings

2. Select a serial port **No.**, and the corresponding serial port type will display automatically.
3. Set **Baud Rate**, **Data Bit**, **Stop Bit** and **Parity**.
4. Set the **Peripheral Type** as **Card Reader**, **QR Code Scanner**, **Fingerprint Module** or **Disable**.

Note

When you select **QR Code Scanner**, **Fingerprint Module** or **Disable**, you can set the peripheral position.

5. You can view the connected device model and peripheral software version.
6. Click **Save**.

Set Wiegand Parameters

You can set the Wiegand transmission direction.

Steps

Note

Some device models do not support this function. Refer to the actual products when configuration.

1. Click **Configuration → Access Control → Wiegand Settings** .
2. Select **Entrance** or **Exit**.
3. Enable **Wiegand** function.
4. The wiegand transmission direction is set **Input** by default.

   Note

   Input: the device can connect a Wiegand card reader.
5. Click **Save** to save the settings.

   Note

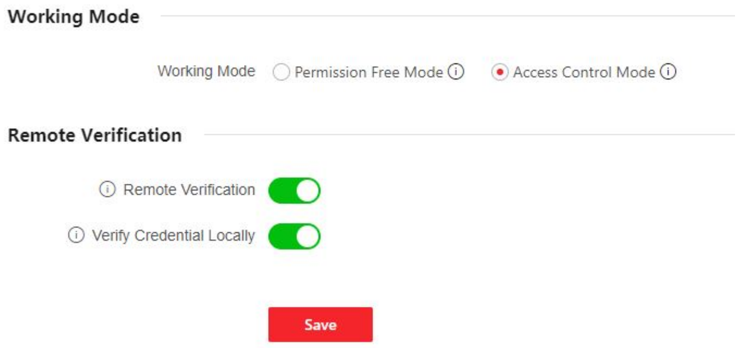
   If you change the peripheral, and after you save the device parameters, the device will reboot automatically.

Set Terminal Parameters

Set the working mode and remote verification.

Steps

1. Click **Configuration → Access Control → Terminal Parameters** to enter the page.



Working Mode

Working Mode ○ Permission Free Mode ⓘ ● Access Control Mode ⓘ

Remote Verification

ⓘ Remote Verification

ⓘ Verify Credential Locally

Figure 7-11 Terminal Parameters

2. Set the device working mode.

   Permission Free Mode

The device will not verify the person's permission, but only the person's validity period. If the person is in the validity period, the barrier will open.

You can enable **Verify Credential Locally**. After enabling the function, the device will only verify the person's permission without the schedule template, etc.

Access Control Mode

The device works normally and will verify the person's permission to open the barrier.

3. Set remote verification.
   1) Enable **Remote Verification**.

   Note

   The device will upload the person's authentication information to the platform. The platform will judge to open the barrier or not.

   2) **Optional:** Enable **Verify Credential Locally**.

   Note

   After enabling the function, the device will only verify the person's permission without the schedule template, etc.

4. Click **Save** to complete terminal parameter settings.

7.6.11 Turnstile

Basic Parameters

Set turnstile basic parameters.

Steps

1. Click **Configuration → Turnstile → Basic Settings** to enter the page.
2. View the **Device Type**, **Device Model** and **Working Status**.
3. Set **Barrier Material**, **Lane Width**, **Barrier Height**, **Barrier Opening Speed** and **Barrier Closing Speed**.
4. Set the passing mode.
   - If you choose **General Passing**, you can select the barrier status for the entrance and exit from the drop-down list.

     Note

     If you set barrier-free mode, the barrier remains open and will close when authentication fails.

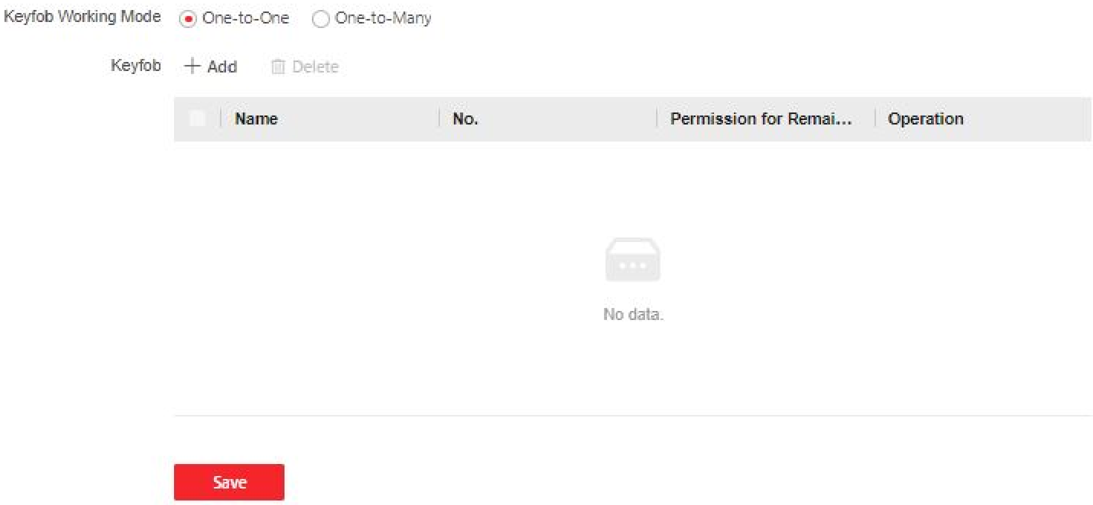
   - If you choose **Weekly Schedule**, you can set a weekly schedule for entrance and exit barriers.
5. Click **Save**.

keyfob

Set keyfob patameters.

Steps

1. Click **Configuration → Turnstile → Keyfob** to enter the page.



Keyfob Working Mode ● One-to-One ○ One-to-Many

Keyfob + Add 🗑 Delete

□	Name	No.	Permission for Remai...	Operation

No data.

Save

Figure 7-12 keyfob

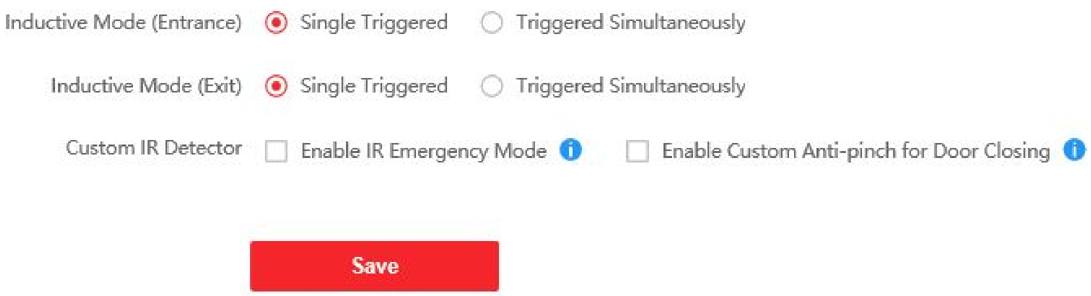
2. Set **Working Mode** as **One-to-One** or **One-to-Many**.
3. Add keyfob.
   1) Click **Add** and the keyfob adding window will pop up.
   2) Enter the **Name** and **Serial No.**.
   3) Check to enable **Remain Open Permission** at your actual needs.
   4) Click **OK** to add the keyfob.
4. **Optional:** Select a keyfob and click **Delete** to delete the keyfob.
5. Click **Save**.

IR Detector

Set IR detector.

Steps

1. Click **Configuration → Turnstile → IR Detector** to enter the page.



Inductive Mode (Entrance) ● Single Triggered ○ Triggered Simultaneously

Inductive Mode (Exit) ● Single Triggered ○ Triggered Simultaneously

Custom IR Detector □ Enable IR Emergency Mode □ Enable Custom Anti-pinch for Door Closing

Figure 7-13 IR Detector

2. Set the entrance and exit inductive mode as **Single Triggered** or **Triggered Simultaneously**.
3. Set custom IR detector mode.

   Enable IR Emergency Mode

      If some IR beams do not work properly, you can shield those IR beams to restore the lane. But this action may hit person and cause injury.

   Enable Custom Anti-pinch for Door Closing

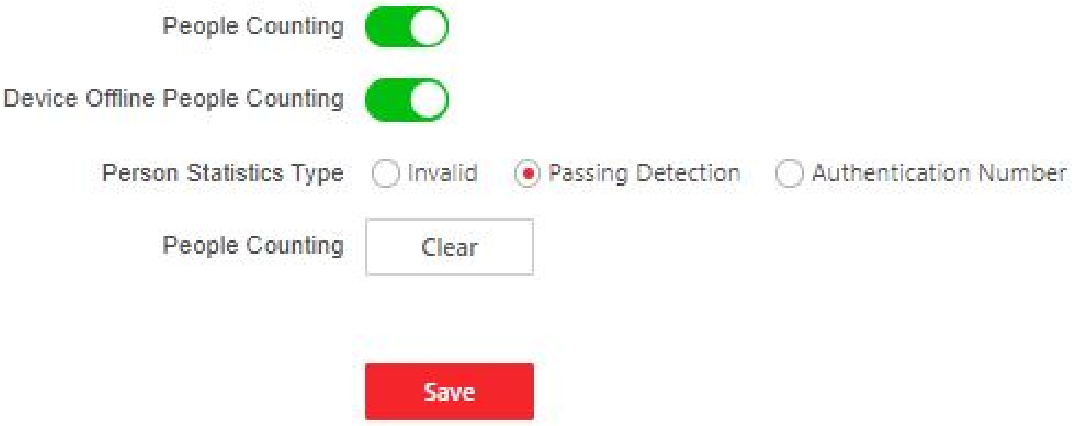
      Anti-pinch for door closing refers that the barrier will not close if the device has detected person in the lane. Only after the person walks out of the lane, the barrier will close. If you enable the function, you can shield parts of the IR beams for closing barrier in advance. But this action may hit person and cause injury.
4. Click **Save**.

People Counting

Set people counting .

Steps

1. Click **Configuration → Turnstile → People Counting** to enter the page.



People Counting ●

Device Offline People Counting ●

Person Statistics Type ○ Invalid ● Passing Detection ○ Authentication Number

People Counting

Figure 7-14 People Counting

2. Check to enable **People Counting**.
3. Enable **Device Offline People Counting** at your actual needs.
4. Select **People Counting Type** as **Invalid**, **Passing Detection** or **Authentication Number**.
5. **Optional:** Click **clear** to clear all the people counting information.

Set Light Color

Set the color for the barrier light.

Steps

1. Click **Configuration → Turnstile → Light Settings** to enter the page.
2. Set barrier light color.
   1) Check to enable **Light on When on Standby** at your actual needs.
   2) Set the barrier light color.
3. Click **Save**.

Other Settings

Set other parameters.

Steps

1. Click **Configuration → Turnstile → Other Settings** to enter the page.
2. Set **Alarm Output Duration**.

   Note

   The alarm output duration ranges from 0 s to 3599 s.
3. Set **Temperature Unit**.

4. Check to enable **Do Not Open Barrier When Lane is Not Clear**.
5. Drag the block or enter the value to adjust the light board brightness.
6. Set the alarm buzzer beeping duration, barrier closing delay time, intrusion duration, overstaying duration and IR obstructed duration.
7. Check to enable **Memory Mode** at your actual needs.

Note

Multiple cards presenting for multiple person passing is allowable when enabling the memory mode. When the passing person's number exceeds the card presenting number, or after the latest person passing with no other person passing within the door open duration, the door will close automatically.

8. Choose the control mode.

   Soft Mode

   The barrier will be closed after the person has passed through the barrier when confronting tailing, forced accessing, etc.

   Guard Mode

   The barrier will be closed immediately when confronting tailgating, forced accessing, etc.
9. Set the fire input type.
10. Click **Save**.

7.6.12 Card Settings

Set Card Security

Click **Configuration → Card Settings → Card Type** to enter the settings page.

Set the parameters and click **Save**.

Enable NFC Card

In order to prevent the mobile phone from getting the data of the access control, you can disable NFC card to increase the security level of the data.

Enable M1 Card

Enable M1 card and authenticating by presenting M1 card is available.

M1 Card Encryption
Sector

M1 card encryption can improve the security level of authentication.

Enable the function and set the encryption sector. By default, Sector 13 is encrypted. It is recommended to encrypt sector 13.

Enable EM Card

Enable EM card and authenticating by presenting EM card is available.

Note

If the peripheral card reader supports presenting EM card, the function is also supported to enable/disable the EM card function.

Enable DESFire Card

The device can read the data from DESFire card when enabling the DESFire card function.

DESFire Card Read Content

After enable the DESFire card content reading function, the device can read the DESFire card content.

Enable FeliCa Card

The device can read the data from FeliCa card when enabling the FeliCa card function.

Set Card Authentication Parameters

Set the card reading content when authenticate via card on the device.

Go to **Configuration → Card Settings → Card NO. Authentication Settings** .

Select a card authentication mode and enable reversed card No. at your actual needs. Click **Save**.

7.6.13 Set Privacy Parameters

Set the event storage type.

Go to **Configuration → Security → Privacy Settings**

The event storage type is overwriting by default. The earliest 5% events will be deleted when the system detects the stored events has been over 95% of the full space.

7.6.14 Set Smart Parameters

Note

Some device models do not support the fingerprint related functions.

Select the card reader at **entrance** or **exit**, and click to enable **Fingerprint Recognition**.

Select **Fingerprint Security Level** from the drop-down list.

Security Level

You can select the fingerprint security level.

The security level related false acceptance rate is shown as below:

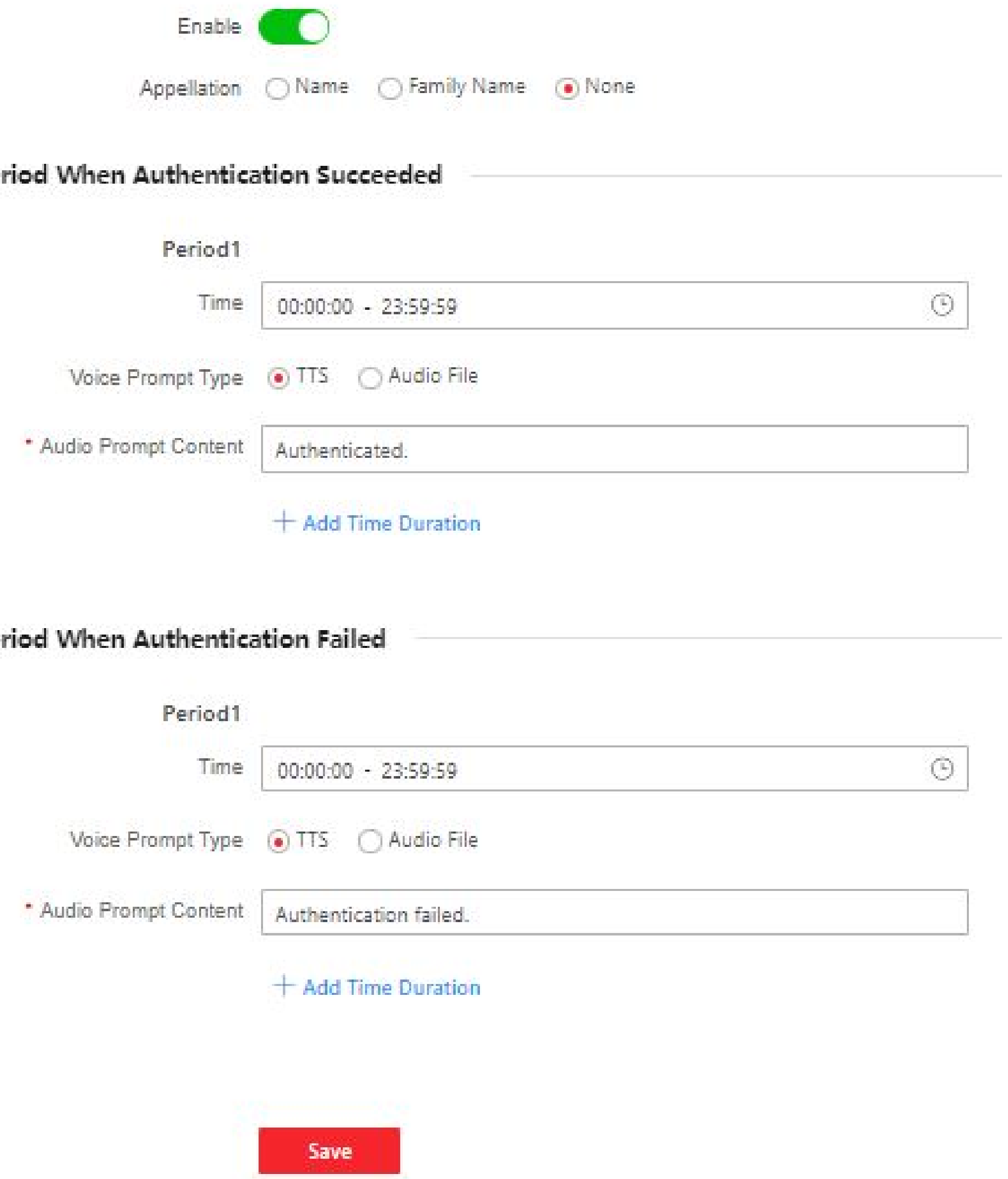
Fingerprint Security Level	False Acceptance Rate (FAR)
3	1/1000 FAR
5	1/100000 FAR
6	1/1000000 FAR
12	3/100000 FAR
13	3/1000000 FAR

7.6.15 Prompt Schedule

Customize the output audio content when authentication succeeded and failed.

Steps

1. Click **Configuration → Preference → Prompt Schedule** .



Enable ●

Appellation ○ Name ○ Family Name ● None

Time Period When Authentication Succeeded

Period1

Time 00:00:00 - 23:59:59

Voice Prompt Type ● TTS ○ Audio File

* Audio Prompt Content Authenticated.

Time Period When Authentication Failed

Period1

Time 00:00:00 - 23:59:59

Voice Prompt Type ● TTS ○ Audio File

* Audio Prompt Content Authentication failed.

Figure 7-15 Customize Audio Content

2. Select time schedule.

3. Enable the function.

4. Set the appellation.

5. Set the time period when authentication succeeded.

1) Click **Add Time Duration**.

2) Set the time duration.

Note

If authentication is succeeded in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication success.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.
5) **Optional:** Click 🗑 to delete the configured time duration.

6. Set the time duration when authentication failed.

1) Click **Add**.
2) Set the time duration.

Note

If authentication is failed in the configured time duration, the device will broadcast the configured content.

3) Set the audio content.

TTS

If you choose TTS, you need to set the language and enter the prompt content of authentication failure.

Audio File

If you choose audio file, you need to select an available audio file from the drop-down list or click **Audio File Management** to add a new file.

Note

The audio file's format should be wav, and the size should be within 200 KB.

4) **Optional:** Repeat substep 1 to 3.
5) **Optional:** Click 🗑 to delete the configured time duration.

7. Click **Save** to save the settings.

7.6.16 Upgrade and Maintenance

Reboot device, restore device parameters, and upgrade device version.

Reboot Device

Click **Maintenance and Security → Maintenance → Restart** .

Click **Restart** to reboot the device.

Upgrade

Click **Maintenance and Security → Maintenance → Upgrade** .

Select an upgrade type from the drop-down list. Click 🗀 and select the upgrade file from your local PC. Click **Upgrade** to start upgrading.

Note

Do not power off during the upgrading.

Restore Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Restore All

All parameters will be restored to the factory settings. You should activate the device before usage.

Restore

The device will restore to the default settings, except for the network parameters and the user information.

Import and Export Parameters

Click **Maintenance and Security → Maintenance → Backup and Reset** .

Export

Click **Export** to export the device parameters.

Note

You can import the exported device parameters to another device.

Import

Click 🗀 and select the file to import. Click **Import** to start import configuration file.

7.6.17 Device Debugging

You can set device debugging parameters.

Steps

1. Click **Maintenance and Security → Maintenance → Device Debugging** .
2. You can set the following parameters.

   Enable SSH

To raise network security, disable SSH service. The configuration is only used to debug the device for the professionals.

Print Log

You can select a component from drop-down list and click **Export** to export log.

Capture Network Packet

You can set the **Capture Packet Duration**, **Capture Packet Size**, and click **Start Capture** to capture.

7.6.18 Component Status

Main Lane Status

Device Component

You can view the status of the access control board, lane control board, main extended interface board, lane status indicator board and IR adapter board.

Peripheral Device

You can view the status of the RS-485 card reader and tamper input.

Temperature

You can view the pedestal temperature.

Movement

You can view the working status of motor encoder.

Sub Lane Status

Device Component

You can view the status of the lane control board, lane status indicator board and IR adapter board.

Peripheral

You can view the status of the RS-485 card reader, RS-232 card receiver and tamper input.

Movement

You can view the working status of motor encoder.

Others

Passing Mode

You can view the passing mode of entrance and exit.

IR Detector Status

You can view the status of each pair of the IR beam sensors.

Input and Output Status

You can view the status of the event input/output, alarm input/output and fire alarm.

Other Status

You can view the status of the barrier and the keyfob receiving module.

7.6.19 Log Query

You can search and view the device logs.

Go to **Maintenance and Security → Maintenance → Log** .

Set the major and minor type of the log type. Set the start time and end time for searching, and click **Search**.

The results will be displayed below, which including the No., time, the major type the minor type, the channel No., the local/remote user information, the remote host IP, etc.

7.6.20 Certificate Management

It helps to manage the server/client certificates and CA certificate.

Note

The function is only supported by certain device models.

Create and Install Self-signed Certificate

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Certificate Files** area, select a **Certificate Type** from the drop-down list.
3. Click **Create**.
4. Input certificate information.
5. Click **OK** to save and install the certificate.

   The created certificate is displayed in the **Certificate Details** area.

   The certificate will be saved automatically.
6. Download the certificate and save it to an asking file in the local computer.
7. Send the asking file to a certification authority for signature.
8. Import the signed certificate.
   1) Select a certificate type in the **Import Passwords** area, and select a certificate from the local, and click **Install**.
   2) Select a certificate type in the **Import Communication Certificate** area, and select a certificate from the local, and click **Install**.

Install Other Authorized Certificate

If you already has an authorized certificate (not created by the device), you can import it to the device directly.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. In the **Import Passwords** and **Import Communication Certificate** areas, select certificate type and upload certificate.
3. Click **Install**.

Install CA Certificate

Before You Start

Prepare a CA certificate in advance.

Steps

1. Go to **Maintenance and Security → Security → Certificate Management** .
2. Create an ID in the **Import CA Certificate** area.

   Note

   The input certificate ID cannot be the same as the existing ones.
3. Upload a certificate file from the local.
4. Click **Install**.

Chapter 8 Client Software Configuration

8.1 Configuration Flow of Client Software

Follow the flow diagram below to configure on the client software.

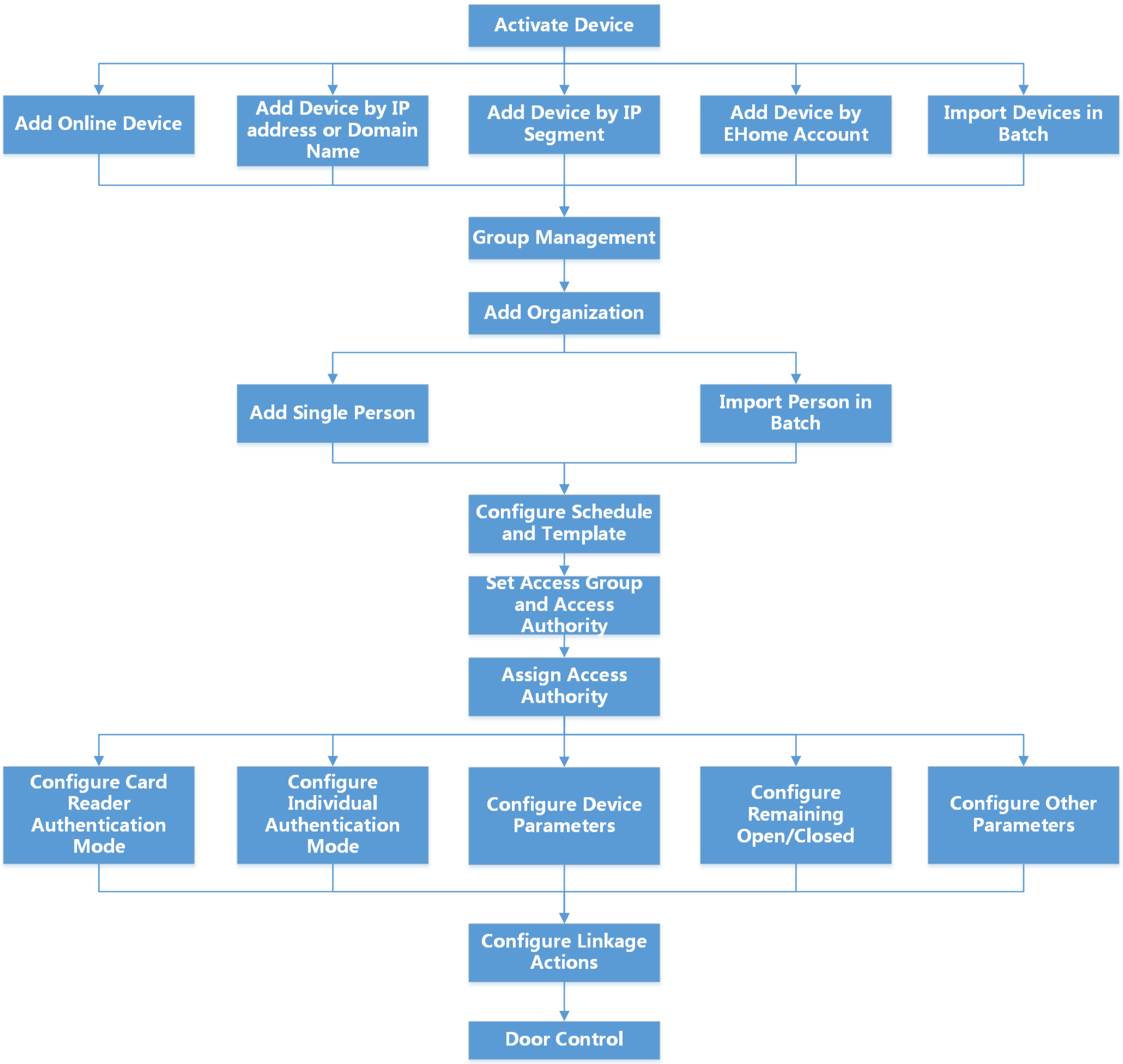

Activate Device
Add Online Device
Add Device by IP address or Domain Name
Add Device by IP Segment
Add Device by EHome Account
Import Devices in Batch
Group Management
Add Organization
Add Single Person
Import Person in Batch
Configure Schedule and Template
Set Access Group and Access Authority
Assign Access Authority
Configure Card Reader Authentication Mode
Configure Individual Authentication Mode
Configure Device Parameters
Configure Remaining Open/Closed
Configure Other Parameters
Configure Linkage Actions
Door Control

Figure 8-1 Flow Diagram of Configuration on Client Software

8.2 Device Management

The client supports managing access control devices and video intercom devices.

Example

You can control entrance & exit and manage attendance after adding access control devices to the client; you can perform video intercom with the indoor stations and door stations.

8.2.1 Add Device

The client provides three device adding modes including by IP/domain, IP segment, and ISUP protocol. The client also supports importing multiple devices in a batch when there are large amount of devices to be added.

Add Device by IP Address or Domain Name

If you know the IP address or domain name of the device to add, you can add devices to the client by specifying the IP address (or domain name), user name, password, etc.

Steps

1. Enter Device Management module.
2. Click **Device** tab on the top of the right panel.

   The added devices are displayed on the right panel.
3. Click **Add** to open the Add window, and then select **IP/Domain** as the adding mode.
4. Enter the required information.

   Name

   Create a descriptive name for the device. For example, you can use a nickname that can show the location or feature of the device.

   Address

   The IP address or domain name of the device.

   Port

   The devices to add share the same port number. The default value is ***80***.

   User Name

   Enter the device user name. By default, the user name is ***admin***.

   Password

   Enter the device password.

   ⚠ **Caution**

   The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

5. **Optional:** Check **Transmission Encryption (TLS)** to enable transmission encryption using TLS (Transport Layer Security) protocol for security purpose.

Note

- This function should be supported by the device.
- If you have enabled Certificate Verification, you should click **Open Certificate Directory** to open the default folder, and copy the certificate file exported from the device to this default directory to strengthen the security.
- You can log into the device to get the certificate file by web browser.

6. Check **Synchronize Time** to synchronize the device time with the PC running the client after adding the device to the client.
7. **Optional:** Check **Import to Group** to create a group by the device name, and import all the channels of the device to this group.

   Example

   For access control device, its access points, alarm inputs/outputs, and encoding channels (if exist) will be imported to this group.
8. Finish adding the device.
   - Click **Add** to add the device and back to the device list page.
   - Click **Add and New** to save the settings and continue to add other device.

Import Devices in a Batch

You can add multiple devices to the client in a batch by entering the device parameters in a pre-defined CSV file.

Steps

1. Enter the Device Management module.
2. Click **Device** tab on the top of the right panel.
3. Click **Add** to open the Add window, and then select **Batch Import** as the adding mode.
4. Click **Export Template** and then save the pre-defined template (CSV file) on your PC.
5. Open the exported template file and enter the required information of the devices to be added on the corresponding column.

   Note

   For detailed description of the required fields, refer to the introductions in the template.

   Adding Mode

   Enter ***0*** or ***1*** or ***2***.

Address

Edit the address of the device.

Port

Enter the device port number. The default port number is ***8000***.

User Name

Enter the device user name. By default, the user name is ***admin***.

Password

Enter the device password.

⚠ **Caution**

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

Import to Group

Enter ***1*** to create a group by the device name. All the channels of the device will be imported to the corresponding group by default. Enter ***0*** to disable this function.

6. Click ⋯ and select the template file.
7. Click **Add** to import the devices.

8.2.2 Reset Device Password

If you forgot the password of the detected online devices, you can reset the device password via the client.

Steps

1. Enter Device Management page.
2. Click **Online Device** to show the online device area.

   All the online devices sharing the same subnet will be displayed in the list.
3. Select the device from the list and click 🔑 on the Operation column.
4. Reset the device password.
   - Click **Generate** to pop up the QR Code window and click **Download** to save the QR code to your PC. You can also take a photo of the QR code to save it to your phone. Send the picture to our technical support.

Note

For the following operations for resetting the password, contact our technical support.

Caution

The password strength of the device can be automatically checked. We highly recommend you change the password of your own choosing (using a minimum of 8 characters, including at least three kinds of following categories: upper case letters, lower case letters, numbers, and special characters) in order to increase the security of your product. And we recommend you change your password regularly, especially in the high security system, changing the password monthly or weekly can better protect your product.

Proper configuration of all passwords and other security settings is the responsibility of the installer and/or end-user.

8.2.3 Manage Added Devices

After adding devices to device list, you can manage the added devices including editing device parameters, remote configuration, viewing device status, etc.

Table 8-1 Manage Added Devices

Edit Device	Click ✎ to edit device information including device name, address, user name, password, etc.
Delete Device	Check one or more devices, and click **Delete** to delete the selected devices.
Remote Configuration	On the device list page, click ⚙ in the Operation column to perform remote configuration for a device. The ⚙ is in the rightmost column of the Device page. For details, refer to the user manual of device.
View Device Status	Click ▤ to view device status, including door No., door status, etc. **Note** For different devices, you will view different information about device status.
View Online User	Click 👤 to view the details of online user who access the device, including user name, user type, IP address and login time.
Refresh Device Information	Click ↻ to refresh and get the latest device information.
Upgrade Device	View device status in the Firmware Upgrade column, check one or more upgradable devices, and click **Upgrade Device Firmware** to upgrade the selected devices. For details, refer to .

Get Events from Device	Check one device, and click **Get Events from Device** to synchronize events. For details, refer to .
Export Device	Click **Export Device**, set the saving path and select device type to export the device details (such as device type, IP address, and port No.) to your local PC. **Note** The super user can enable **Password Protection** and enter the password, then the exported file of device information will be encrypted.

8.3 Group Management

The client provides groups to manage the added resources in different groups. You can group the resources into different groups according to the resources' locations.

Example
For example, on the 1st floor, there mounted 16 doors, 64 alarm inputs, and 16 alarm outputs. You can organize these resources into one group (named 1st Floor) for convenient management. You can control door status, and do some other operations of the devices after managing the resources by groups.

8.3.1 Add Group

You can add group to organize the added device for convenient management.

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Create a group.
   - Click **Add Group** and enter a group name as you want.
   - Click **Create Group by Device Name** and select an added device to create a new group by the name of the selected device.

   Note

   The resources (such as alarm inputs/outputs, access points, etc.) of this device will be imported to the group by default.

8.3.2 Import Resources to Group

You can import the device resources (such as alarm inputs/outputs, access points, etc.) to the added group in a batch.

Before You Start

Add a group for managing devices. Refer to ***Add Group*** .

Steps

1. Enter the Device Management module.
2. Click **Device Management → Group** to enter the group management page.
3. Select a group from the group list and select the resource type as **Access Point**, **Alarm Input**, **Alarm Output**, etc.
4. Click **Import**.
5. Select the thumbnails/names of the resources in the thumbnail/list view.

   Note

   You can click ⊞ or ☰ to switch the resource display mode to thumbnail view or to list view.
6. Click **Import** to import the selected resources to the group.

8.4 Person Management

You can add person information to the system for further operations such as access control, video intercom, time and attendance, etc. You can manage the added persons such as issuing cards to them in a batch, importing and exporting person information in a batch, etc.

8.4.1 Add Organization

You can add an organization and import person information to the organization for effective management of the persons. You can also add a surbodinate organization for the added one.

Steps

1. Enter **Person** module.
2. Select a parent organization in the left column and click **Add** in the upper-left corner to add an organization.
3. Create a name for the added organization.

   Note

   Up to 10 levels of organizations can be added.
4. **Optional:** Perform the following operation(s).

   Edit Organization Hover the mouse on an added organization and click ✎ to edit its name.

Delete Organization

Hover the mouse on an added organization and click × to delete it.

Note

- The lower-level organizations will be deleted as well if you delete an organization.
- Make sure there is no person added under the organization, or the organization cannot be deleted.

Show Persons in Sub Organization

Check **Show Persons in Sub Organization** and select an organization to show persons in its sub organizations.

8.4.2 Configure Basic Information

You can add person to the client one by one and configure the person's basic information such as name, email, phone number, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person.
3. Click **Add** to open the adding person window.

   The Person ID will be generated automatically.
4. Enter the basic information including person name, telephone number, email address, validity period, etc.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

8.4.3 Issue a Card by Local Mode

If a card enrollment station is available, you can issue a card by local mode. To read the card number, you should connect the card enrollment station to the PC running the client by USB interface or COM, and place the card on the card enrollment station.

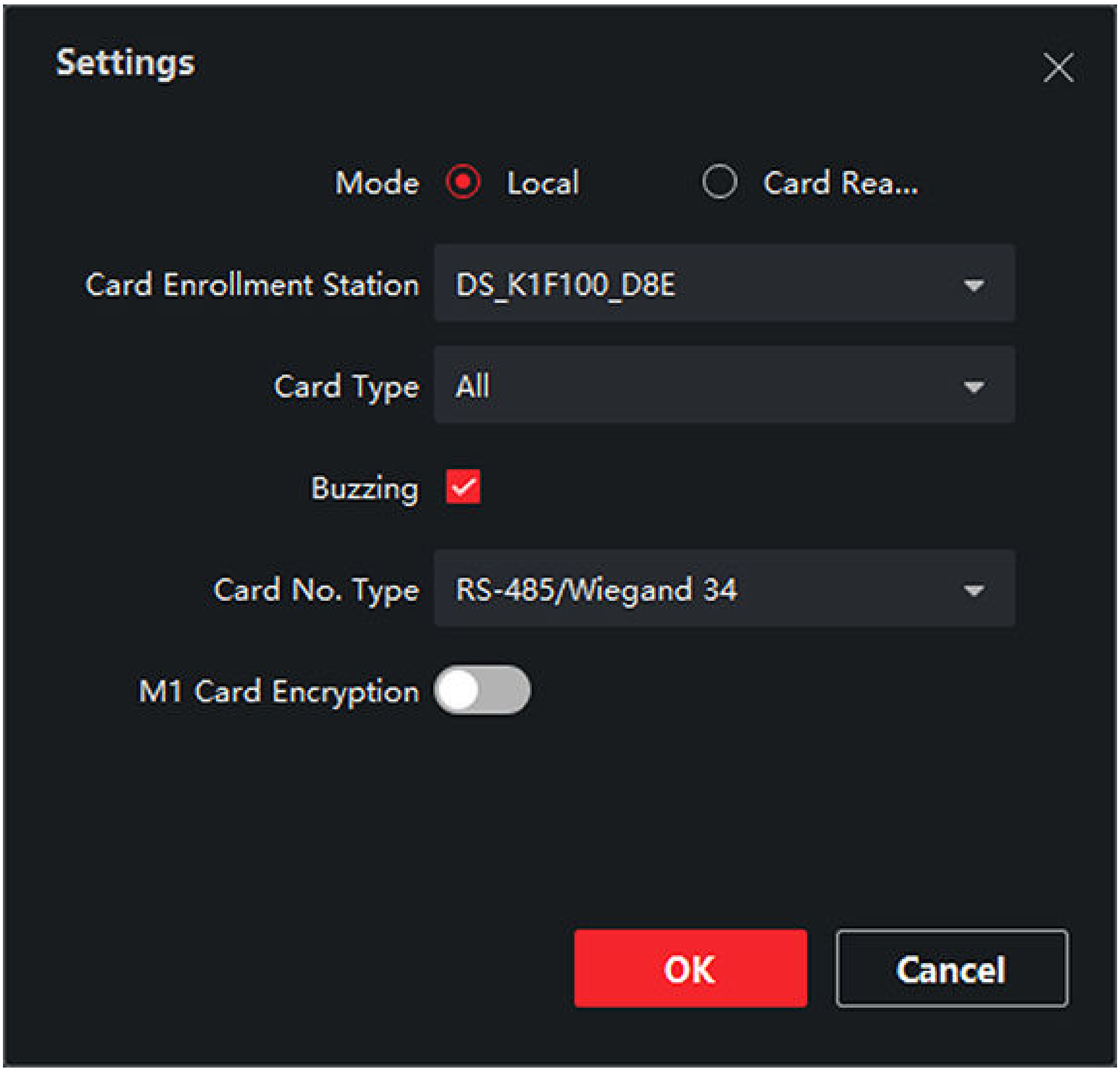
Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person panel.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. In the **Credential → Card** area, click **+**.

4. Click **Settings** to enter the Settings page.
5. Select **Local** as the card issuing mode.



Settings

Mode ● Local ○ Card Rea...

Card Enrollment Station: DS_K1F100_D8E

Card Type: All

Buzzing ☑

Card No. Type: RS-485/Wiegand 34

M1 Card Encryption

Figure 8-2 Issue a Card by Local Mode

6. Set other related parameters.

   Card Enrollment Station

   Select the model of the connected card enrollment station.

   Note

   Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

   Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E. Select the card type as EM card or M1 card according to the actual card type.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E. If the card is M1 card, then you can enable the M1 Card Encryption function and select the sector of the card to encrypt.

7. Click **OK** to confirm the operation.
8. Place the card on the card enrollment station, and click **Read** to get the card number.

   The card number will display in the Card No. field automatically.
9. Click **Add**.

   The card will be issued to the person.

8.4.4 Upload a Face Photo from Local PC

When adding person, you can upload a face photo stored in local PC to the client as the person's profile.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information panel.
4. Select **Upload**.
5. Select a picture from the PC running the client.

   Note

   The picture should be in JPG or JPEG format and smaller than 200 KB.
6. **Optional:** Enable **Verify by Device** to check whether the facial recognition device managed in the client can recognize the face in the photo.

   Note

   This function is hidden or shown according to the device capacity.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.

- Click **Add and New** to add the person and continue to add other persons .

8.4.5 Take a Photo via Client

When adding a person, you can take a photo of the her/him via the client and set this photo as the person's profile.

Before You Start

Make sure PC running the client has a camera or you have connected other USB camera to the PC.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add** to enter Add Person window.

   Note

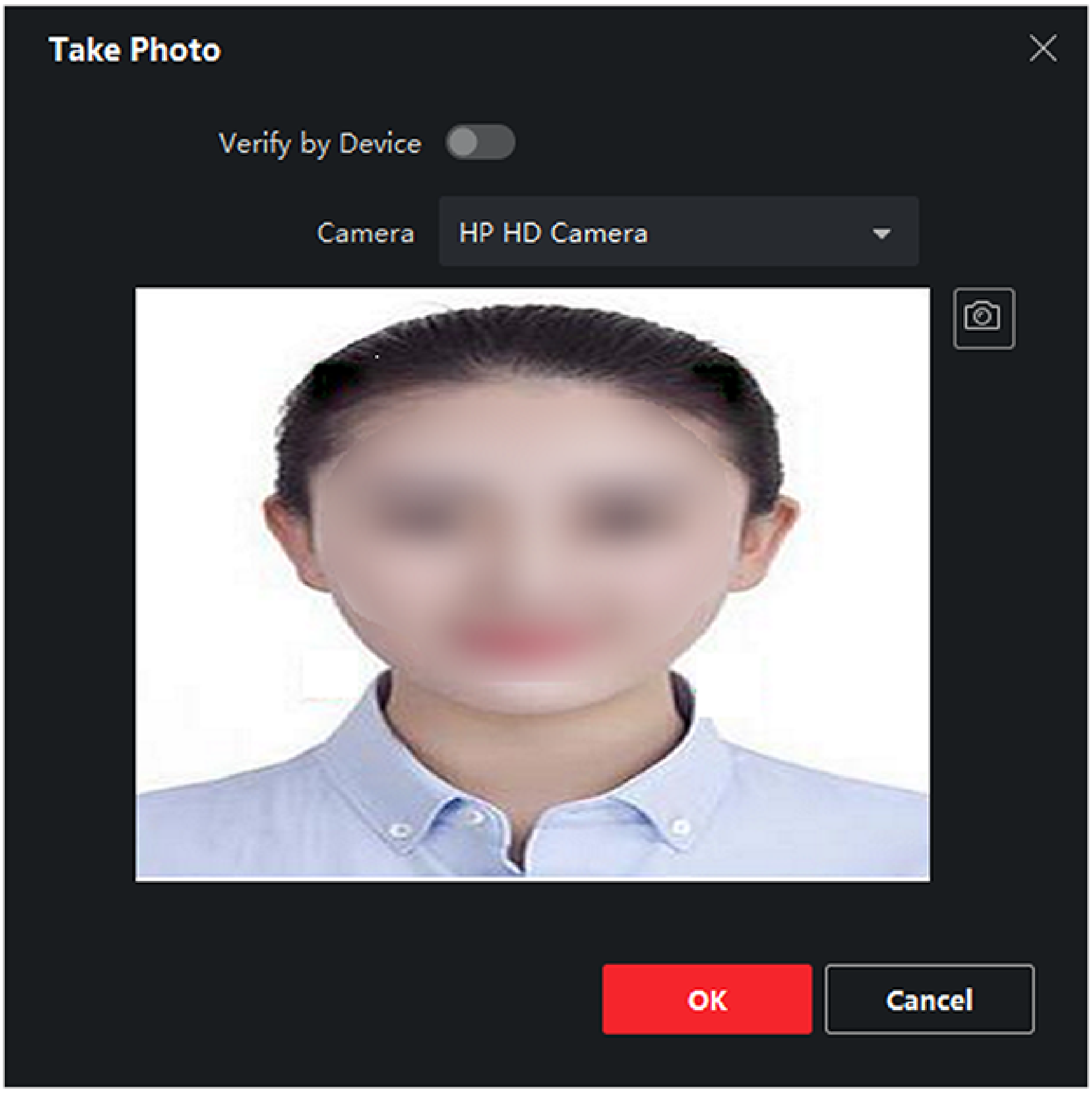
   Enter the person's basic information first. For details, refer to ***Configure Basic Information*** .
3. Click **Add Face** in the Basic Information area.
4. Select **Take Photo** to enter Take Photo window.
5. **Optional:** Enable **Verify by Device** to check whether the captured face photo can meet the uploading requirements.
6. Take a photo.

   1) Face to the camera and make sure your face is in the middle of the collecting window.

   2) Click 📷 to capture a face photo.

   3) **Optional:** Click ↻ to capture again.

   4) Click **OK** to save the captured photo.



Take Photo

Verify by Device

Camera: HP HD Camera

Figure 8-3 Take a Photo via Client

7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

8.4.6 Collect Face via Access Control Device

When adding person, you can collect the person's face via access control device added to the client which supports facial recognition function.

Steps

1. Enter **Person** module.

2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. Click **Add Face** in the Basic Information panel.
4. Select **Remote Collection**.
5. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login** to set related parameters of the device including IP address, port No., user name, and password. Also, you can check **Face Anti-Spoofing** and select the liveness level as Low, Medium, or High.

   Face Anti-Spoofing

   If you check this function, then the device can detect whether the face to be collected is an authentic one.

6. Collect face.
   1) Face to the camera of the selected access control device and make sure your face is in the middle of the collecting window.
   2) Click 📷 to capture a photo.
   3) Click **OK** to save the captured photo.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

8.4.7 Collect Fingerprint via Client

Collecting fingerprints locally means you can collect the fingerprint via the fingerprint recorder connected directly to the PC running the client. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Connect the fingerprint recorder to the PC running the client.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Local**.

5. Select the model of the connected fingerprint recorder.

Note

If the fingerprint recorder is DS-K1F800-F, you can click **Settings** to select the COM the fingerprint recorder connects to.

6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint recorder to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

Note

Once the fingerprint is added, the fingerprint type cannot be changed.

8.4.8 Collect Fingerprint via Access Control Device

When adding person, you can collect fingerprint information via the access control device's fingerprint module. The fingerprints recorded can be used as credentials of the persons to access the authorized doors.

Before You Start

Make sure fingerprint collection is supported by the access control device.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Credential → Fingerprint** panel, click **+**.
4. In the pop-up window, select the collection mode as **Remote**.
5. Select an access control device which supports fingerprint recognition function from the drop-down list.
6. Collect the fingerprint.
   1) Click **Start**.
   2) Place and lift your fingerprint on the fingerprint scanner of the selected access control device to collect the fingerprint.
   3) Click **Add** to save the recorded fingerprint.
7. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.

- Click **Add and New** to add the person and continue to add other persons .

Note

Once the fingerprint is added, the fingerprint type cannot be changed.

8.4.9 Configure Access Control Information

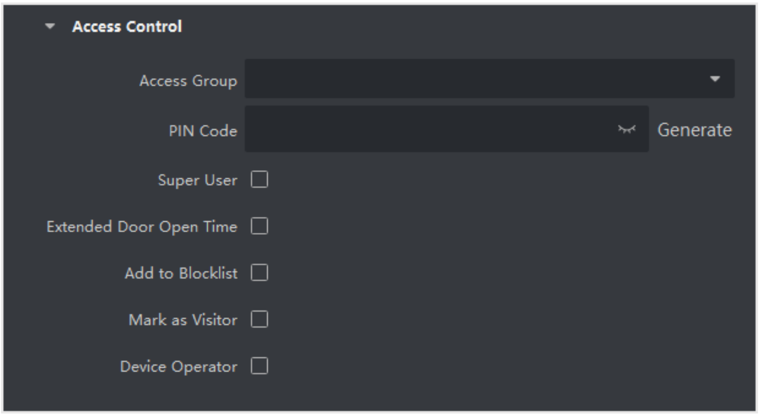
When adding a person, you can set her/his access control information, such as binding an access control group with the person, configuring PIN code, setting the person as a visitor, a blocklist person, or a super user, etc.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.
3. In the **Access Control** area, click to select access group(s) for the person.

Note

For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .



Access Control

Access Group

PIN Code Generate

Super User □

Extended Door Open Time □

Add to Blocklist □

Mark as Visitor □

Device Operator □

Figure 8-4 Configure Access Control Information

4. Set a unique PIN code for the person which can be used for access authentication.
   - Manually enter a PIN code containing 4 to 8 digits.

     Note

     Persons' PIN codes cannot be repeated.
   - Click **Generate** to randomly generate an unrepeated PIN code of 6 digits.

     Note

     If there are repeated PIN codes, a prompt will pop up on the client. The admin can generate a new PIN code to replace the repeated PIN code and notify related persons.
5. Check the person's operation permissions.

Super User

If the person is set as a super user, he/she will have authorization to access all the doors/ floors and will be exempted from remaining closed restrictions, all anti-passback rules, and first person authorization.

Extended Door Open Time

Use this function for persons with reduced mobility. When accessing the door, the person will have more time than others to pass through doors.

For details about setting the door's open duration, refer to ***Configure Parameters for Door*** .

Add to Blocklist

Add the person to the blocklist and when the person tries to access doors/floors, an event will be triggered and sent to the client to notify the security personnel.

Mark as Visitor

If the person is a visitor, you should set the her/his valid times for visit.

Note

The valid times for visit is between 1 and 100. You can also check **No Limit**, then there are no limited times for the visitor to access doors/floors.

Device Operator

For person with device operator role, he/she is authorized to operate on the access control devices.

Note

The Super User, Extended Door Open Time, Add to Blocklist, and Mark as Visitor functions cannot be enabled concurrently. For example, if one person is set as super user, you cannot enable extended door open time for her/him, add her/him to the blocklist, or set her/him as visitor.

6. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

8.4.10 Customize Person Information

You can customize the person properties which are not pre-defined in the client according to actual needs, e.g., place of birth. After customizing, when add a person, you can enter the custom information to make the person information complete.

Steps

1. Enter **Person** module.
2. Set the fields of custom information.
   1) Click **Custom Property**.
   2) Click **Add** to add a new property.

3) Enter the property name.
4) Click **OK**.

3. Set the custom information when adding a person.
   1) Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

   2) In the **Custom Information** panel, enter the person information.
   3) Click **Add** to add the person and close the Add Person window, or click **Add and New** to add the person and continue to add other persons.

8.4.11 Configure Resident Information

If the person is resident, for video intercom purpose, you need to set the room number for her/him and bind an indoor station. After bound, you can call this person by calling the indoor station and perform video intercom with her/him.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

   Note

   Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Resident Information** panel, select the indoor station to bind it to the person.

   Note

   If you select **Analog Indoor Station**, the **Door Station** field will display and you are required to select the door station to communicate with the analog indoor station.

4. Enter the floor No. and room No. of the person.
5. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons.

8.4.12 Configure Additional Information

When adding person, you can configure the additional information for the person, such as person's identity type, identity No., country, etc., according to actual needs.

Steps

1. Enter **Person** module.
2. Select an organization in the organization list to add the person and click **Add**.

Note

Enter the person's basic information first. For details about configuring person's basic information, refer to ***Configure Basic Information*** .

3. In the **Additional Information** panel, enter the additional information of the person, including person's ID type, ID No., job title, etc., according to actual needs.
4. Confirm to add the person.
   - Click **Add** to add the person and close the Add Person window.
   - Click **Add and New** to add the person and continue to add other persons .

8.4.13 Import and Export Person Identify Information

You can import the information and pictures of multiple persons to the client software in a batch. Meanwhile, you can also export the person information and pictures and save them in your PC.

8.4.14 Import Person Information

You can enter the information of multiple persons in a predefined template (CSV/Excel file) to import the information to the client in a batch.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel.
4. Select **Person Information** as the importing mode.
5. Click **Download Template for Importing Person** to download the template.
6. Enter the person information in the downloaded template.

Note

- If the person has multiple cards, separate the card No. with semicolon.
- Items with asterisk are required.
- By default, the Hire Date is the current date.

7. Click ··· to select the CSV/Excel file with person information from local PC.
8. Click **Import** to start importing.

Note

- If a person No. already exists in the client's database, delete the existing information before importing.
- You can import information of no more than 2,000 persons.

8.4.15 Import Person Pictures

After importing face pictures for the added persons to the client, the persons in the pictures can be identified by an added face recognition terminal. You can either import person pictures one by one, or import multiple pictures at a time according to your need.

Before You Start
Be sure to have imported person information to the client beforehand.

Steps

1. Enter the Person module.
2. Select an added organization in the list, or click **Add** in the upper-left corner to add an organization and then select it.
3. Click **Import** to open the Import panel and check **Face**.
4. **Optional:** Enable **Verify by Device** to check whether face recognition device managed in the client can recognize the face in the photo.
5. Click ··· to select a face picture file.

   Note

   - The (folder of) face pictures should be in ZIP format.
   - Each picture file should be in JPG format and should be no larger than 200 KB.
   - Each picture file should be named as "Person ID_Name". The Person ID should be the same with that of the imported person information.

6. Click **Import** to start importing.

   The importing progress and result will be displayed.

8.4.16 Export Person Information

You can export the added persons' information to local PC as a CSV/Excel file.

Before You Start
Make sure you have added persons to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' information will be exported if you do not select any organization.

3. Click **Export** to open the Export panel.
4. Check **Person Information** as the content to export.
5. Check desired items to export.
6. Click **Export** to save the exported file in CSV/Excel file on your PC.

8.4.17 Export Person Pictures

You can export face picture file of the added persons and save in your PC.

Before You Start
Make sure you have added persons and their face pictures to an organization.

Steps

1. Enter the Person module.
2. **Optional:** Select an organization in the list.

   Note

   All persons' face pictures will be exported if you do not select any organization.
3. Click **Export** to open the Export panel and check **Face** as the content to export.
4. Click **Export** to start exporting.

   Note

   - The exported file is in ZIP format.
   - The exported face picture is named as "Person ID_Name_0" ("0" is for a full-frontal face).

8.4.18 Get Person Information from Access Control Device

If the added access control device has been configured with person information (including person details, fingerprint, and issued card information), you can get the person information from the device and import them to the client for further operations.

Steps

Note

- If the person name stored in the device is empty, the person name will be filled with the issued card No. after importing to the client.
- If the card number or person ID (employee ID) stored on the device already exists in the client database, the person with this card number or person ID will not be imported to the client.

1. Enter **Person** module.
2. Select an organization to import the persons.
3. Click **Get from Device**.
4. Select an added access control device or the enrollment station from the drop-down list.

   Note

   If you select the enrollment station, you should click **Login**, and set IP address, port No., user name and password of the device.
5. Click **Import** to start importing the person information to the client.

Note

Up to 2,000 persons and 5,000 cards can be imported.

The person information, including person details, person's fingerprint information (if configured), and the linked cards (if configured), will be imported to the selected organization.

8.4.19 Move Persons to Another Organization

You can move the added persons to another organization if you need.

Before You Start

- Make sure you have added at least two organizations.
- Make sure you have imported person information.

Steps

1. Enter **Person** module.
2. Select an organization in the left panel.

   The persons under the organization will be displayed in the right panel.
3. Select the person to move.
4. Click **Change Organization**.
5. Select the organization to move persons to.
6. Click **OK**.

8.4.20 Issue Cards to Persons in Batch

The client provides a convenient way to issue cards to multiple persons in a batch.

Steps

1. Enter **Person** module.
2. Click **Batch Issue Cards**.

   All the added persons with no card issued will be displayed in the right panel.
3. **Optional:** Enter key words (name or person ID) in the input box to filter the person(s) that need issuing cards.
4. **Optional:** Click **Settings** to set the card issuing parameters. For details, refer to *Issue a Card by Local Mode*.
5. Click **Initialize** to initialize the card enrollment station or card reader to make it ready for issuing cards.
6. Click the **Card No.** column and enter the card number.
   - Place the card on the card enrollment station.
   - Swipe the card on the card reader.
   - Manually enter the card number and press the **Enter** key.

   The person(s) in the list will be issued with card(s).

8.4.21 Report Card Loss

If the person lost his/her card, you can report the card loss so that the card's related access authorization will be inactive.

Steps

1. Enter **Person** module.
2. Select the person you want to report card loss for and click **Edit** to open the Edit Person window.
3. In the **Credential → Card** panel, click on the added card to set this card as lost card.

   After reporting card loss, the access authorization of this card will be invalid and inactive. Other person who gets this card cannot access the doors by swiping this lost card.
4. **Optional:** If the lost card is found, you can click to cancel the loss.

   After cancelling card loss, the access authorization of the person will be valid and active.
5. If the lost card is added in one access group and the access group is applied to the device already, after reporting card loss or cancelling card loss, a window will pop up to notify you to apply the changes to the device. After applying to device, these changes can take effect on the device.

8.4.22 Set Card Issuing Parameters

The client provides two modes for reading a card's number: via card enrollment station or via the card reader of the access control device. If a card enrollment station is available, connect it to the PC running the client by USB interface or COM, and place the card on the card enrollment to read the card number. If not, you can also swipe the card on the card reader of the added access control device to get the card number. As a result, before issuing a card to one person, you need to set the card issuing parameters including the issuing mode and related parameters.

When adding a card to one person, click **Settings** to open the Card Issuing Settings window.

Local Mode: Issue Card by Card Enrollment Station

Connect a card enrollment station to the PC running the client. You can place the card on the card enrollment station to get the card number.

Card Enrollment Station

Select the model of the connected card enrollment station

Note

Currently, the supported card enrollment station models include DS-K1F100-D8, DS-K1F100-M, DS-K1F100-D8E, and DS-K1F180-D8E.

Card Type

This field is only available when the model is DS-K1F100-D8E or DS-K1F180-D8E.

Select the card type as EM card or IC card according to the actual card type.

Serial Port

It is only available when the model is DS-K1F100-M.

Select the COM the card enrollment station connects to.

Buzzing

Enable or disable the buzzing when the card number is read successfully.

Card No. Type

Select the type of the card number according to actual needs.

M1 Card Encryption

This field is only available when the model is DS-K1F100-D8, DS-K1F100-D8E, or DS-K1F180-D8E.

If the card is M1 card, and if you need to enable the M1 Card Encryption function, you should enable this function and select the sector of the card to encrypt.

Remote Mode: Issue Card by Card Reader

Select an access control device added in the client and swipe the card on its card reader to read the card number.

8.5 Configure Schedule and Template

You can configure the template including holiday and week schedule. After setting the template, you can adopt the configured template to access groups when setting the access groups, so that the access group will take effect in the time durations of the template.

Note

For access group settings, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

8.5.1 Add Holiday

You can create holidays and set the days in the holidays, including start date, end date, and holiday duration in one day.

Steps

Note

You can add up to 64 holidays in the software system.

1. Click **Access Control → Schedule → Holiday** to enter the Holiday page.
2. Click **Add** on the left panel.
3. Create a name for the holiday.
4. **Optional:** Enter the descriptions or some notifications of this holiday in the Remark box.
5. Add a holiday period to the holiday list and configure the holiday duration.

Note

Up to 16 holiday periods can be added to one holiday.

1) Click **Add** in the Holiday List field.
2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

   Up to 8 time durations can be set to one holiday period.
3) **Optional:** Perform the following operations to edit the time durations.
   - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
   - Click the time duration and directly edit the start/end time in the appeared dialog.
   - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⟺ .
4) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
5) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
6) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.

6. Click **Save**.

8.5.2 Add Template

Template includes week schedule and holiday. You can set week schedule and assign the time duration of access authorization for different person or group. You can also select the added holiday(s) for the template.

Steps

Note

You can add up to 255 templates in the software system.

1. Click **Access Control → Schedule → Template** to enter the Template page.

   Note

   There are two default templates: All-Day Authorized and All-Day Denied, and they cannot be edited or deleted.

   All-Day Authorized

   The access authorization is valid in each day of the week and it has no holiday.

   All-Day Denied

The access authorization is invalid in each day of the week and it has no holiday.

2. Click **Add** on the left panel to create a new template.
3. Create a name for the template.
4. Enter the descriptions or some notification of this template in the Remark box.
5. Edit the week schedule to apply it to the template.
   1) Click **Week Schedule** tab on the lower panel.
   2) Select a day of the week and draw time duration(s) on the timeline bar.

   Note

   Up to 8 time duration(s) can be set for each day in the week schedule.

   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .

   4) Repeat the two steps above to draw more time durations on the other days of the week.
6. Add a holiday to apply it to the template.

   Note

   Up to 4 holidays can be added to one template.

   1) Click **Holiday** tab.
   2) Select a holiday in the left list and it will be added to the selected list on the right panel.
   3) **Optional:** Click **Add** to add a new holiday.

   Note

   For details about adding a holiday, refer to ***Add Holiday*** .

   4) **Optional:** Select a selected holiday in the right list and click ✕ to remove the selected one, or click **Clear** to clear all the selected holiday(s) in the right list.
7. Click **Save** to save the settings and finish adding the template.

8.6 Set Access Group to Assign Access Authorization to Persons

After adding the person and configuring the person's credentials, you can create the access groups to define which person(s) can get access to which door(s) and then apply the access group to the access control device to take effect.

Before You Start

- Add person to the client.
- Add access control device to the client and group access points. For details, refer to ***Group Management*** .
- Add template.

Steps

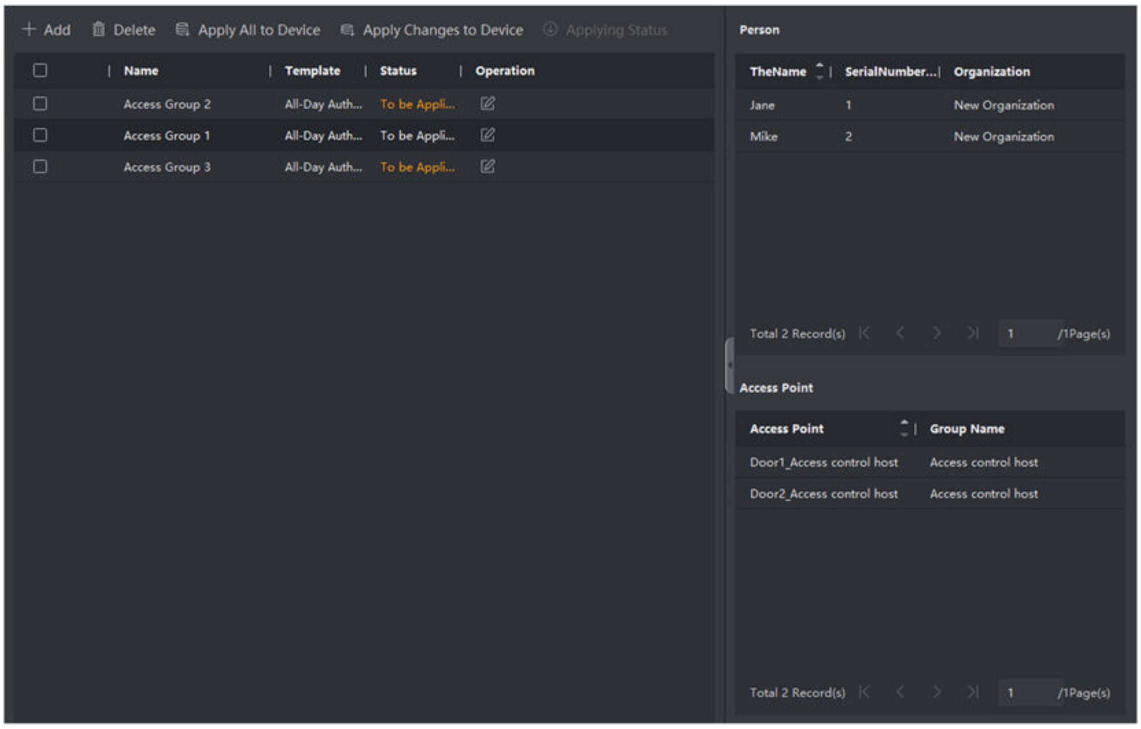
When the access group settings are changed, you need to apply the access groups to the devices again to take effect. The access group changes include changes of template, access group settings, person's access group settings, and related person details (including card number, fingerprint, face picture, linkage between card number and fingerprint, linkage between card number and fingerprint, card password, card effective period, etc).

1. Click **Access Control → Authorization → Access Group** to enter the Access Group interface.
2. Click **Add** to open the Add window.
3. In the **Name** text field, create a name for the access group as you want.
4. Select a template for the access group.

   Note

   You should configure the template before access group settings. Refer to ***Configure Schedule and Template*** for details.
5. In the left list of the Select Person field, select person(s) to assign access authority.
6. In the left list of the Select Access Point field, select door(s), door station(s) or floor(s) for the selected persons to access.
7. Click **Save**.

   You can view the selected person(s) and the selected access point(s) on the right side of the interface.



□	Name	Template	Status	Operation
□	Access Group 2	All-Day Auth...	To be Appli...	✎
□	Access Group 1	All-Day Auth...	To be Appli...	✎
□	Access Group 3	All-Day Auth...	To be Appli...	✎

Person

TheName	SerialNumber...	Organization
Jane	1	New Organization
Mike	2	New Organization

Total 2 Record(s) 1 /1Page(s)

Access Point

Access Point	Group Name
Door1_Access control host	Access control host
Door2_Access control host	Access control host

Total 2 Record(s) 1 /1Page(s)

Figure 8-5 Display the Selected Person(s) and Access Point(s)

8. After adding the access groups, you need to apply them to the access control device to take effect.
   1) Select the access group(s) to apply to the access control device.
   2) Click **Apply All to Devices** start applying all the selected access group(s) to the access control device or door station.
   3) Click **Apply All to Devices** or **Apply Changes to Devices**.

      Apply All to Devices

      This operation will clear all the existed access groups of the selected devices and then apply the new access group to the device.

      Apply Changes to Devices

      This operation will not clear the existed access groups of the selected devices and only apply the changed part of the selected access group(s) to the device(s).
   4) View the applying status in the Status column or click **Applying Status** to view all the applied access group(s).

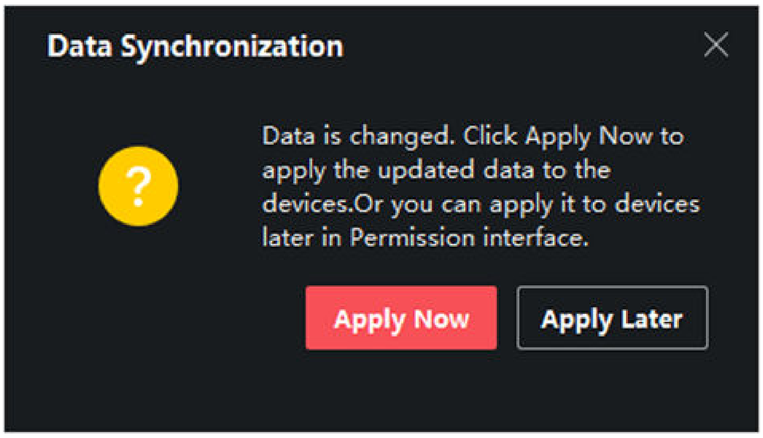
   Note

   You can check **Display Failure Only** to filter the applying results.

   The selected persons in the applied access groups will have the authorization to enter/exit the selected doors/door stations with their linked card(s) or fingerprints.
9. **Optional:** Click ✎ to edit the access group if necessary.

Note

If you change the persons' access information or other related information, you will view the prompt **Access Group to Be Applied** on the right corner of the client.
You can click the prompt to apply the changed data to the device. You can select either **Apply Now** or **Apply Later**.



Data Synchronization

Data is changed. Click Apply Now to apply the updated data to the devices.Or you can apply it to devices later in Permission interface.

Figure 8-6 Data Synchronization

8.7 Configure Advanced Functions

You can configure the advanced functions of access control to meet some special requirements in different scene.

Note

- For the card related functions(the type of access control card), only the card(s) with access group applied will be listed when adding cards.
- The advanced functions should be supported by the device.
- Hover the cursor on the Advanced Function, and then Click ⚙ to customize the advanced function(s) to be displayed.

8.7.1 Configure Device Parameters

After adding the access control device, you can configure the parameters of access control device, access control points.

Configure Parameters for Access Control Device

After adding the access control device, you can configure its parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .

   Note

   If you can find Device Parameter in the Advanced Function list, Hover the cursor on the Advanced Function, and then Click ⚙ to select the Device Parameter to be displayed.

2. Select an access device to show its parameters on the right page.
3. Turn the switch to ON to enable the corresponding functions.

   Note

   The displayed parameters may vary for different access control devices.

   RS-485 Communication Redundancy

   You should enable this function if you wire the RS-485 card reader to the access control device redundantly.

   Enable NFC

   If enable the function, the device can recognize the NFC card. You can present NFC card on the device.

   Enable M1 Card

   If enable the function, the device can recognize the M1 card. You can present M1 card on the device.

   Enable EM Card

   If enable the function, the device can recognize the EM card. You can present EM card on the device.

   Enable CPU Card

   Reserved. If enable the function, the device can recognize the CPU card. You can present CPU card on the device.

   Enable ID Card

   Reserved. If enable the function, the device can recognize the ID card. You can present ID card on the device.

4. Click **OK**.
5. **Optional:** Click **Copy to**, and then select the access control device(s) to copy the parameters in the page to the selected device(s).

Configure Parameters for Door

After adding the access control device, you can configure its access point door parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .

2. Select an access control device on the left panel, and then click ▸ to show the doors or floors of the selected device.
3. Select a door or floor to show its parameters on the right page.
4. Edit the door or floor parameters.

Note

s
The displayed parameters may vary for different access control devices.

Name

Edit the card reader name as desired.

Exit Button Type

You can set the exit button as remaining closed or remaining open. Usually, it is remaining open.

Open Duration

After swiping the normal card and relay action, the time for locking the door starts working.

Door Left Open Timeout Alarm

The alarm can be triggered if the door has not been closed in a configured time period. If it is set as 0, no alarm will be triggered.

Super Password

The specific person can open the door by inputting the super password.

5. Some of the following parameters are not listed in the Basic Information page, click **Advanced** to edit the parameters.

Duress Code

The door can open by inputting the duress code when there is duress. At the same time, the client can report the duress event.

Dismiss Code

Create a dismiss code which can be used to stop the buzzer of the card reader (by entering the dismiss code on the keypad).

Note

- The duress code, super code, and dismiss code should be different.
- The duress code, super password, and the dismiss code should be different from the authentication password.
- The length of duress code, super password, and the dismiss code is according the device, usually it should contains 4 to 8 digits.

6. Click **OK**.
7. **Optional:** Click **Copy to** , and then select the door(s) to copy the parameters in the page to the selected doors(s).

Note

The door's status duration settings will be copied to the selected door(s) as well.

Configure Parameters for Card Reader

After adding the access control device, you can configure its card reader parameters.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** .
2. In the device list on the left, click ▸ to expand the door, select a card reader and you can edit the card reader's parameters on the right.
3. Edit the card reader basic parameters in the Basic Information page.

   Note

   The displayed parameters may vary for different access control devices. There are part of parameters listed as follows. Refer to the user manual of the device for more details.

   Name

   Edit the card reader name as desired.

   Minimum Card Swiping Interval

   If the interval between card swiping of the same card is less than the set value, the card swiping is invalid. You can set it as 0 to 255.

   Alarm of Max. Failed Attempts

   Enable to report alarm when the card reading attempts reach the set value.

   Card Reader Type/Card Reader Description

   Get card reader type and description. They are read-only.
4. **Optional:** Some of the following parameters are not listed in the Basic Information page, click **Advanced** to edit the parameters.

   Enable Card Reader

   If enabling the function, user can present card on the card reader. If disabling the function, the card reader for entrance cannot be used.

   OK LED Polarity/Error LED Polarity/Buzzer Polarity

   Set OK LED Polarity/Error LED Polarity/Buzzer LED Polarity of main board according to the card reader parameters. Generally, adopts the default settings.

   Buzzing Time

   Set the card reader buzzing time. The available time ranges from 0 to 5,999s. 0 represents continuous buzzing.

   Max. Interval When Entering PWD

When you inputting the password on the card reader, if the interval between pressing two digits is larger than the set value, the digits you pressed before will be cleared automatically.

Tampering Detection

Enable the anti-tamper detection for the card reader.

Communicate with Controller Every

When the access control device cannot connect with the card reader for longer than the set time, the card reader will turn offline automatically.

Fingerprint Recognition Level

Select the fingerprint recognition level in the drop-down list.

5. Click **OK**.
6. **Optional:** Click **Copy to**, and then select the card reader(s) to copy the parameters in the page to the selected card reader(s).

Configure Parameters for Alarm Output

After adding the access control device, if the device links to alarm outputs, you can configure the parameters.

Before You Start

Add access control device to the client, and make sure the device supports alarm output.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter access control parameter configuration page.
2. In the device list on the left, click ▸ to expand the door, select an alarm input and you can edit the alarm input's parameters on the right.
3. Set the alarm output parameters.

   Name

   Edit the card reader name as desired.

   Alarm Output Active Time

   How long the alarm output will last after triggered.
4. Click **OK**.
5. **Optional:** Set the switch on the upper right corner to **ON** to trigger the alarm output.

Configure Parameters for Lane Controller

After adding the lane controller to the client, you can configure its parameters for passing through the lane.

Steps

1. Click **Access Control → Advanced Function → Device Parameter** to enter Parameter Settings page.
2. In the device list on the left, select a lane controller and you can edit the lane controller's parameters on the right.
3. Edit the parameters.

   Passing Mode

   Select the controller which will control the barrier status of the device.

   - If you select **According to DIP Settings**, the device will follow the controller's DIP settings to control the barrier. The settings on the software will be invalid.
   - If you select **According to Door's Schedule Settings**, the device will follow the schedule configured in the client software to control the barrier. The DIP settings of the controller will be invalid.

   Enable Free Passing Authentication

   After enabling free passing authentication, an alarm will be triggered when the passing personnel has no permission to pass through.

   Opening/Closing Barrier Speed

   Set the barrier's opening and closing speed. You can select from 1 to 10. The greater the value, the faster the speed.

   Note

   The recommended value is 6.

   Alarm Voice Prompt Duration

   Set how long the audio will last, which is played when an alarm is triggered.

   Note

   0 refers to the alarm audio will be played until the alarm is ended.

   Temperature Unit

   Select the temperature unit that displayed in the device status.

   Lightboard Brightness

   Set the lightboard brightness.

   Barrier Material

   Select the material of the barrier gate. You can select the barrier material from the drop-down list.

   Note

   The barrier material will affect the device working. Select a correct barrier material or the barrier may not open.

Lane Length

The width of the lane. You can set the lane width.

Note

The lane width will affect the device working. Set a correct lane width or the barrier may not open.

Do Not Open Barrier When Lane is Not Clear

If there is someone or something in the lane, the gate will not open even if the credential is authenticated.

This function is designed to avoid more than one person passing through the gate with only one authentication.

4. Click **OK**.

8.7.2 Configure Remaining Open/Closed

You can set the status of the door as open or closed. For example, you can set the door remaining closed in the holiday, and set the door remaining open in the specified period of the work day.

Before You Start

Add the access control devices to the system.

Steps

1. Click **Access Control → Advanced Function → Remain Open/Closed** to enter the Remain Open/ Closed page.
2. Select the door that need to be configured on the left panel.
3. To set the door status during the work day, click the **Week Schedule** and perform the following operations.
   1) Click **Remain Open** or **Remain Closed**.
   2) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

   Up to 8 time durations can be set to each day in the week schedule.

   3) **Optional:** Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to ✋ .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
   4) Click **Save**.

   Related Operations

Copy to Whole Week Select one duration on the time bar, click **Copy to Whole Week** to copy all the duration settings on this time bar to other week days.

Delete Selected Select one duration on the time bar, click **Delete Selected** to delete this duration.

Clear Click **Clear** to clear all the duration settings in the week schedule.

4. To set the door status during the holiday, click the **Holiday** and perform the following operations.
   1) Click **Remain Open** or **Remain Closed**.
   2) Click **Add**.
   3) Enter the start date and end date.
   4) Drag the cursor to draw the time duration, which means in that duration of time, the configured access group is activated.

   Note

   Up to 8 time durations can be set to one holiday period.

   5) Perform the following operations to edit the time durations.
      - Move the cursor to the time duration and drag the time duration on the timeline bar to the desired position when the cursor turns to 🖐 .
      - Click the time duration and directly edit the start/end time in the appeared dialog.
      - Move the cursor to the start or the end of time duration and drag to lengthen or shorten the time duration when the cursor turns to ⇔ .
   6) **Optional:** Select the time duration(s) that need to be deleted, and then click ⊗ in the Operation column to delete the selected time duration(s).
   7) **Optional:** Click 🗑 in the Operation column to clear all the time duration(s) in the time bar.
   8) **Optional:** Click ☒ in the Operation column to delete this added holiday period from the holiday list.
   9) Click **Save**.
5. **Optional:** Click **Copy to** to copy the door status settings of this door to other door(s).

8.7.3 Configure Multi-Factor Authentication

You can manage the persons by group and set the authentication for multiple persons of one access control point (door).

Before You Start

Set access group and apply the access group to the access control device. For details, refer to ***Set Access Group to Assign Access Authorization to Persons*** .

Perform this task when you want to set authentications for multiple cards of one access control point (door).

Steps

1. Click **Access Control → Advanced Function → Multi-Factor Auth** .
2. Select an access control device in device list on the left panel.

3. Add a person/card group for the access control device.
   1) Click **Add** on the right panel.
   2) Create a name for the group as desired.
   3) Specify the start time and end time of the effective period for the person/card group.
   4) Select members(s) and card(s) in the Available list, and the selected member(s) and card(s) will be added to the Selected list.

   Note

   Make sure you have issue card to the person.
   Make sure you have set access group and apply the access group to the access control device successfully.

   5) Click **Save**.
   6) **Optional:** Select the person/card group(s), and then click **Delete** to delete it(them).
   7) **Optional:** Select the person/card group(s), and then click **Apply** to re-apply access group that failed to be applied previously to the access control device.
4. Select an access control point (door) of selected device on the left panel.
5. Enter the maximum interval when entering password.
6. Add an authentication group for the selected access control point.
   1) Click **Add** on the Authentication Groups panel.
   2) Select a configured template as the authentication template from the drop-down list.

   Note

   For setting the template, refer to ***Configure Schedule and Template*** .

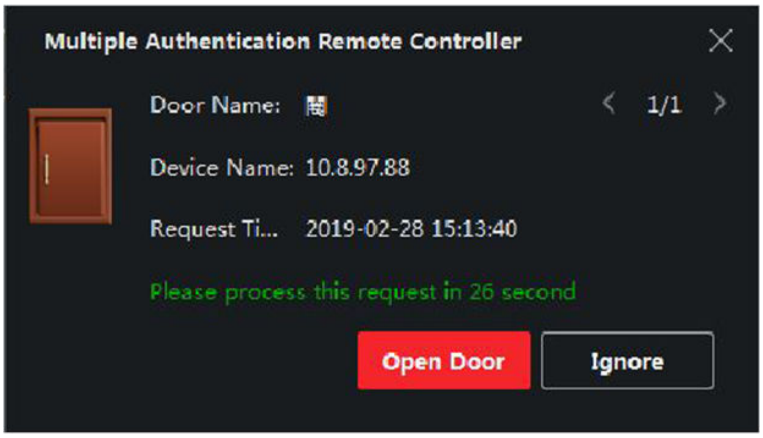
   3) Select the authentication type as **Local Authentication**, **Local Authentication and Remotely Open Door**, or **Local Authentication and Super Password** from the drop-down list.

   Local Authentication

   Authentication by the access control device.

   Local Authentication and Remotely Open Door

   Authentication by the access control device and by the client. When the person swipes the card on the device, a window will pop up. You can unlock the door via the client.



Multiple Authentication Remote Controller

Door Name:

Device Name: 10.8.97.88

Request Ti... 2019-02-28 15:13:40

Please process this request in 26 second

Figure 8-7 Remotely Open Door

Note

You can check **Offline Authentication** to enable the super password authentication when the access control device is disconnected with the client.

Local Authentication and Super Password

Authentication by the access control device and by the super password.

4) Select the added person/card group in the left list below and it will be added to the Selected list on the right as the authentication group.

5) Click the added authentication group in the right list to set authentication times in the Auth Times column.

Note

- The authentication times should be larger than 0 and smaller than the added personnel quantity in the personnel group.
- The maximum value of authentication times is 16.

6) Click **Save**.

Note

- For each access control point (door), up to four authentication groups can be added.
- For the authentication group of which authentication type is **Local Authentication**, up to 8 person/card groups can be added to the authentication group.
- For the authentication group of which authentication type is **Local Authentication and Super Password** or **Local Authentication and Remotely Open Door**, up to 7 person/card groups can be added to the authentication group.

7. Click **Save**.

8.7.4 Configure Custom Wiegand Rule

Based on the knowledge of uploading rule for the third party Wiegand, you can set multiple customized Wiegand rules to communicate between the device and the third party card readers.

Before You Start

Wire the third party card readers to the device.

Steps

Note

- By default, the device disables the custom wiegand function. If the device enables the custom Wiegand function, all wiegand interfaces in the device will use the customized wiegand protocol.
- Up to 5 custom Wiegands can be set.
- For details about the custom Wiegand, see Custom Wiegand Rule Descriptions.

1. Click **Access Control → Advanced Function → Custom Wiegand** to enter the Custom Wiegand page.
2. Select a custom Wiegand on the left.
3. Create a Wiegand name.

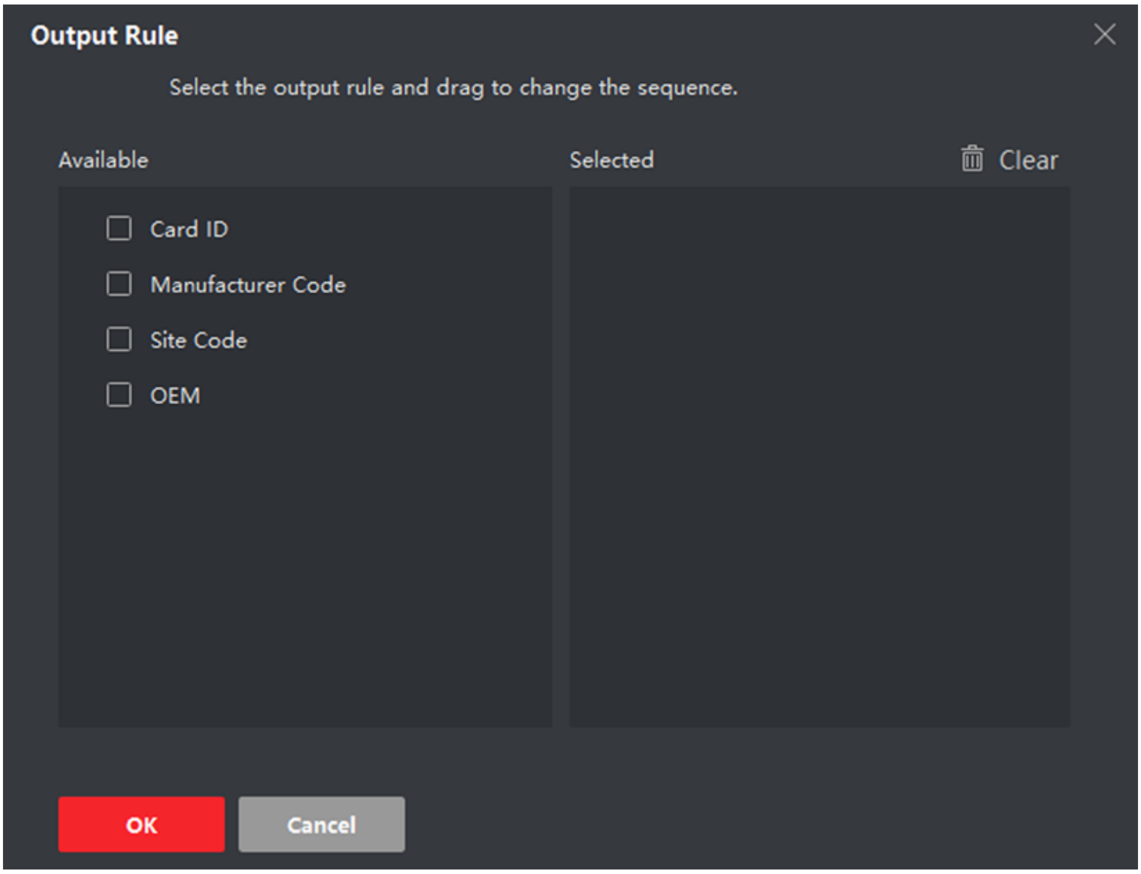
   Note

   Up to 32 characters are allowed in the custom Wiegand name.
4. Click **Select Device** to select the access control device for setting the custom wiegand.
5. Set the parity mode according to the property of the third party card reader.

   Note

   - Up to 80 bits are allowed in the total length.
   - The odd parity start bit, the odd parity length, the even parity start bit and the even parity length range from 1 to 80 bit.
   - The start bit of the card ID, the manufacturer code, the site code, and the OEM should range from 1 to 80 bit.
6. Set output transformation rule.

   1) Click **Set Rule** to open the Set Output Transformation Rules window.



Output Rule

Select the output rule and drag to change the sequence.

Available

- □ Card ID
- □ Manufacturer Code
- □ Site Code
- □ OEM

Selected

Figure 8-8 Set Output Transformation Rule

2) Select rules on the left list.

The selected rules will be added to the right list.

3) **Optional:** Drag the rules to change the rule order.

4) Click **OK**.

5) In the Custom Wiegand tab, set the rule's start bit, length, and the decimal digit.

7. Click **Save**.

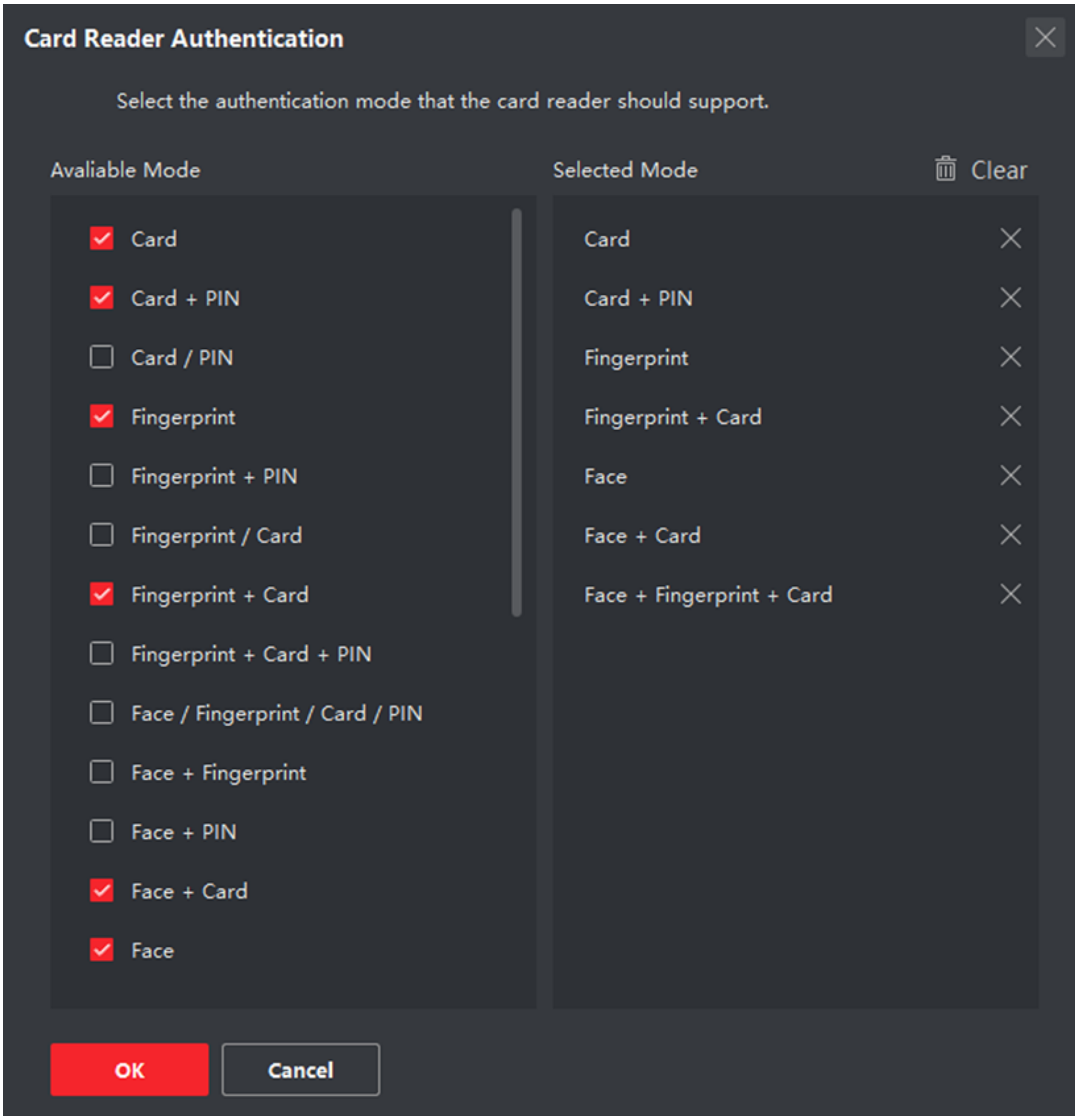
8.7.5 Configure Card Reader Authentication Mode and Schedule

You can set the passing rules for the card reader of the access control device according to your actual needs.

Steps

1. Click **Access Control → Advanced Function → Authentication** to enter the authentication mode configuration page.
2. Select a card reader on the left to configure.
3. Set card reader authentication mode.

   1) Click **Configuration**.



Card Reader Authentication

Select the authentication mode that the card reader should support.

Avaliable Mode

☑ Card
☑ Card + PIN
□ Card / PIN
☑ Fingerprint
□ Fingerprint + PIN
□ Fingerprint / Card
☑ Fingerprint + Card
□ Fingerprint + Card + PIN
□ Face / Fingerprint / Card / PIN
□ Face + Fingerprint
□ Face + PIN
☑ Face + Card
☑ Face

Selected Mode

Clear

Card ✕
Card + PIN ✕
Fingerprint ✕
Fingerprint + Card ✕
Face ✕
Face + Card ✕
Face + Fingerprint + Card ✕

OK

Cancel

Figure 8-9 Select Card Reader Authentication Mode

Note

PIN refers to the PIN code set to open the door. Refer to ***Configure Access Control Information*** .

2) Check the modes in the Available Mode list and they will be added to the selected modes list.

3) Click **OK**.

After selecting the modes, the selected modes will display as icons with different color.

4. Click the icon to select a card reader authentication mode, and drag the cursor to draw a color bar on the schedule, which means in that period of time, the card reader authentication is valid.
5. Repeat the above step to set other time periods.

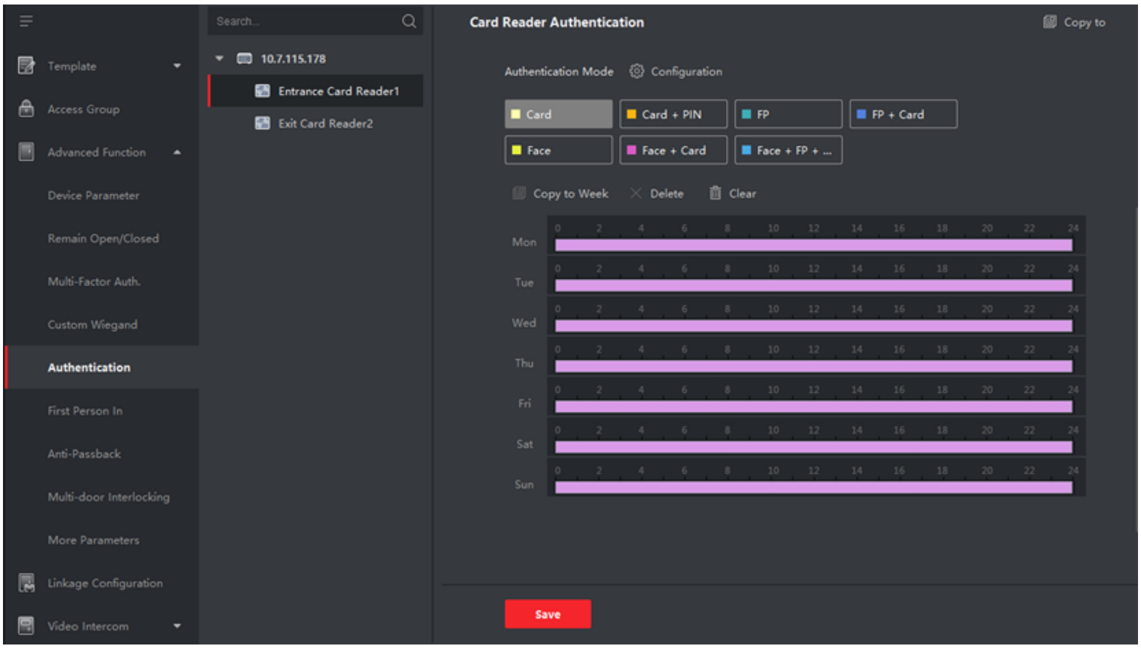


Figure 8-10 Set Authentication Modes for Card Readers

6. **Optional:** Select a configured day and click **Copy to Week** to copy the same settings to the whole week.
7. **Optional:** Click **Copy to** to copy the settings to other card readers.
8. Click **Save**.

8.7.6 Configure First Person In

You can set multiple first persons for one access control point. After the first person is authorized, it allows multiple persons access the door or other authentication actions.

Before You Start

- Add access control device to the client, and make sure the device supports the first person in function.
- Add person and assign access authorization to designed person. For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .

Steps

1. Click **Access Control → Advanced Function → First Person In** to enter the First Person In page.
2. Select an access control device in the list on the left panel.
3. Select the current mode as **Enable Remaining Open after First Person**, **Disable Remaining Open after First Person**, or **Authorization by First Person** from the drop-down list for each access control point of the selected device.

   Enable Remaining Open after First Person

The door remains open for the configured time duration after the first person is authorized until the remain open duration ends. If you select this mode, you should set the remain open duration.

Note

The remain open duration should be between 0 and 1440 minutes. By default, the remain open duration is 10 minutes.

Disable Remaining Open after First Person

Disable the function of first person in, namely normal authentication.

Authorization by First Person

All authentications (except for the authentications of super card, super password, duress card, and duress code) are allowed only after the first person authorization.

Note

You can authenticate by the first person again to disable the first person mode.

4. Click **Add** on the First Person List panel.
5. Select person(s) in the left list and the person(s) will be add to the selected persons as the first person(s) of the doors.

   The added first person(s) will list in the First Person List
6. **Optional:** Select a first person from the list and click **Delete** to remove the person from the first person list.
7. Click **Save**.

8.7.7 Configure Anti-Passback

The anti-passback feature is designed to minimizes the misuse or fraudulent use of access credentials such as passing back card to an unauthorized person, or tailed access. The anti-passback function establishes a specific sequence in which access credentials must be used in order to grant access. You can set the sequence according to the actual path via the client and if the person uses the credential in wrong sequence, you can also reset the anti-password records.

Before You Start

Add access control device to the client, and enable the anti-passing back function of the access control device.

Steps

Note

Either the anti-passing back or multi-door interlocking function can be configured for an access control device at the same time. For the configuration of multi-door interlocking, refer to .

1. Click **Access Control → Advanced Function → Anti-Passback** to enter the Anti-Passpack Settings page.

2. Select an access control device on the left panel.
3. Select a card reader as the beginning of the path in the **First Card Reader** field.
4. Click ✎ of the selected first card reader in the **Card Reader Afterward** column to open the select card reader dialog.
5. Select the afterward card readers for the first card reader.

Note

Up to four afterward card readers can be added as afterward card readers for one card reader.

6. Click **OK** in the dialog to save the selections.
7. Click **Save** in the Anti-Passback Settings page to save the settings and take effect.

Example

Set Card Swiping Path: If you select Reader In_01 as the beginning, and select Reader In_02, Reader Out_04 as the linked card readers. Then you can only get through the access control point by swiping the card in the order as Reader In_01, Reader In_02 and Reader Out_04.

8. Click **Reset Anti-Passback** and select the person(s) to delete the related anti-passback records about the person(s) on the device.

Note

This function should be supported by the device.

8.7.8 Configure Device Parameters

After adding the access control device, you can set its parameters such as network parameters.

Set RS-485 Parameters

You can set the access control device's RS-485 parameters including the baud rate, data bit, the stop bit, parity type, flow control type, communication mode, work mode, and connection mode.

Steps

Note

The RS-485 Settings should be supported by the device.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **RS-485** to enter the RS-485 Settings page.
4. Select the serial port number from the drop-down list to set the RS-485 parameters.
5. Set the serial number, external device, authentication center, baud rate, data bit, stop bit, parity type, flow control type, communication mode, and working mode in the drop-down list.
6. Click **Save**.

- The configured parameters will be applied to the device automatically.
- When you change the working mode or connection mode, the device will reboot automatically.

Enable M1 Card Encryption

M1 card encryption can improve the security level of authentication.

Steps

Note

The function should be supported by the access control device and the card reader.

1. Enter the Access Control module.
2. On the navigation bar on the left, enter **Advanced Function → More Parameters** .
3. Select an access control device in the device list and click **M1 Card Encryption** to enter the M1 Card Encryption page.
4. Set the switch to on to enable the M1 card encryption function.
5. Set the sector ID.

   The sector ID ranges from 1 to 100.
6. Click **Save** to save the settings.

8.8 Configure Linkage Actions for Access Control

You can configure different linkage actions for the event detected by the access control device. After that, linkage actions will be triggered once the event happens. This mechanism is used for notifying the security personnel the event, or triggering automatic access control in real time.

Two types of linkage actions are supported:

- **Client Actions:** When the event is detected, it will trigger the actions on the client, such as the client making an audible warning..
- **Device Actions:** When the event is detected, it will trigger the actions of a specific device, such as buzzing of a card reader and, opening/closing of a door, ..

8.8.1 Configure Client Actions for Access Event

Even if you are far away from an access point, you can still know what happens and how urgent the event is via the client by configuring client actions for the access event. Client actions here refer to the actions automatically executed by the client itself, such as making an audible warning and sending an email. Once an event is triggered, the client will notify the security personnel, so that he/she can handle the event in time.

Before You Start

Add access control device to the client.

Steps

1. Click **Event Configuration → Access Control Event** .

   The added access control devices will display in the device list.
2. Select a resource (including device, alarm input, door, and card reader) from the device list.

   The event types which the selected resource supports appear.
3. Select the event(s) and click **Edit Priority** to define the priority for the event(s), which can be used to filter events in the Event Center.
4. Set the linkage actions of the event.

   1) Select the event(s) and click **Edit Linkage** to set the client actions when the event(s) are triggered.

      Audible Warning

      The client software gives an audible warning when the event is triggered. You can select alarm sound for the audible warning.

      Note

      For details about setting the alarm sound, refer to *Set Alarm Sound* in the user manual of the client software.

      Send Email

      Send an email notification about the event to one or more receivers.

      For details about setting email parameters, refer to *Set Email Parameters* in the user manual of the client software.

   2) Click **OK**.
5. Enable the event so that when the event is detected, event will be sent to the client and the linkage actions will be triggered.
6. **Optional:** Click **Copy to** to copy the event settings to other access control device, alarm input, door, or card reader.

8.8.2 Configure Device Actions for Access Event

You can set the access control device's linkage actions for the access control device's triggered event. When the event is triggered, it can trigger the alarm output, host buzzer, and other actions on the same device.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .

2. Select the access control device from the list on the left.
3. Click **Add** button to add a new linkage.
4. Select the event source as **Event Linkage**.
5. select the event type and detailed event to set the linkage.
6. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.
7. Click **Save**.
8. **Optional:** After adding the device linkage, you can do one or more of the following:

Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.
Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.

8.8.3 Configure Device Actions for Card Swiping

You enable access control device's linkage actions (such as disarming a zone and triggering audio prompt) for the swiping of a specific card, In this way, you can monitor the card holder's behaviors and whereabouts.

Steps

Note

It should be supported by the device.

1. Click **Access Control → Linkage Configuration** .
2. Select the access control device from the list on the left.
3. Click **Add** to add a new linkage.
4. Select **Card Linkage** as the event source.
5. Enter the card number or select the card from the drop-down list.
6. Select the card reader where the card swipes.
7. In the Linkage Target area, set the property target to enable this action.

   Buzzer on Controller

   The audible warning of access control device will be triggered.

   Buzzer on Reader

   The audible warning of card reader will be triggered.

   Capture

   An event-related picture will be captured when the selected event happens.

   Recording

An event-related picture will be captured when the selected event happens.

Note

The device should support recording.

Alarm Output

The alarm output will be triggered for notification.

Alarm Input

Arm or disarm the alarm input.

Note

The device should support alarm input function.

Access Point

The door status of open, close, remain open, or remain closed will be triggered.

Audio Play

The audio prompt will be triggered. And the select audio index related audio content will be played according to the configured play mode.

8. Click **Save**.

   When the card (configured in Step 5) swipes on the card reader (configured in Step 6), it can trigger the linked actions (configured in step 7).

9. **Optional:** After adding the device linkage, you can do one or more of the followings:

Delete Linkage Settings	Select the configured linkage settings in the device list and click **Delete** to delete it.
Edit Linkage Settings	Select the configured linkage settings in the device list and you can edit its event source parameters, including event source and linkage target.

8.9 Door Control

In Monitoring module, you can view the real-time status of the doors managed by the added access control device. You can also control the doors such as open/close the door, or remain the door open/closed via the client remotely. The real-time access event are displayed in this module. You can view the access details and person details.

Note

For the user with door control permission, the user can enter the Monitoring module and control the door. Or the icons used for control will not show. For setting the user permission, refer to ***Person Management*** .

8.9.1 Control Door Status

You can control the status for the door(s), including unlock door, locking door, remaining the door unlock, remaining the door locked, remain all unlocked, etc.

Before You Start

- Add person and assign access authorization to designed person, and person will have the access authorization to the access points (doors). For details, refer to ***Person Management*** and ***Set Access Group to Assign Access Authorization to Persons*** .
- Make sure the operation user has the permission of the access points (doors).

Steps

1. Click **Monitoring** to enter the status monitoring page.
2. Select an access point group on the upper-right corner.

   Note

   For managing the access point group, refer to ***Group Management*** .

   The doors in the selected access control group will display.
3. Click a door icon to select a door, or press **Ctrl** and select multiple doors.

   Note

   For **Remain All Unlocked** and **Remain All Locked**, ignore this step.
4. Click the following buttons to control the door.

   Unlock

   When the door is locked, unlock it and it will be open for once. After the open duration, the door will be closed and locked again automatically.

   Lock

   When the door is unlocked, lock it and it will be closed. The person who has the access authorization can access the door with credentials.

   Remain Unlocked

   The door will be unlocked (no matter closed or open). All the persons can access the door with no credentials required.

   Remain Locked

   The door will be closed and locked. No person can access the door even if he/she has the authorized credentials, except the super users.

   Remain All Unlocked

   All doors in the group will be unlocked (no matter closed or open). All the persons can access the doors with no credentials required.

   Remain All Locked

All doors in the group will be closed and locked. No person can access the doors even if he/she has the authorized credentials, except the super users.

Capture

Capture a picture manually.

Note

The **Capture** button is available when the device supports capture function. The picture is saved in the PC running the client. For setting the saving path, refer to *Set File Saving Path* in the user manual of the client software.

Result

The icon of the doors will change in real-time according to the operation if the operation is succeeded.

8.9.2 Check Real-Time Access Records

The real-time access records can be displayed in the client, including card swiping records, face recognition records, skin-surface temperature information, etc. Also, you can view the person information and view the picture captured during access.

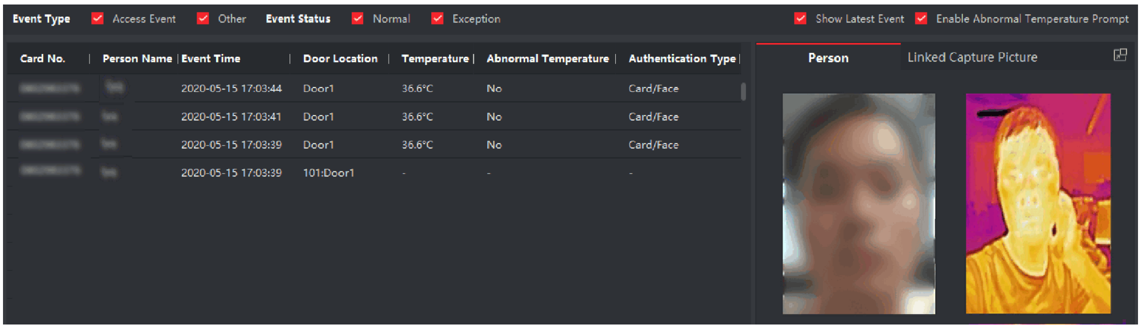
Before You Start

You have added person(s) and access control device(s) to the client. For details, refer to ***Person Management*** and ***Add Device*** .

Steps

1. Click **Monitoring** to enter monitoring module.

   Real-time access records are displayed on the bottom of the page. You can view record details, including card No., person name, event time, door location, temperature, authentication type etc.



Event Type ☑ Access Event ☑ Other **Event Status** ☑ Normal ☑ Exception ☑ Show Latest Event ☑ Enable Abnormal Temperature Prompt

Card No.	Person Name	Event Time	Door Location	Temperature	Abnormal Temperature	Authentication Type
[redacted]	[redacted]	2020-05-15 17:03:44	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:41	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:39	Door1	36.6°C	No	Card/Face
[redacted]	[redacted]	2020-05-15 17:03:39	101:Door1	-	-	-

Figure 8-11 Real-time Access Records

Note

You can right click the column name of access event table to show or hide the column according to actual needs.

2. **Optional:** Select an access point group from the drop-down list in the upper-right corner to show the real time access records of the selected group.
3. **Optional:** Check the event type and event status.

   The detected events of checked type and status will be displayed in the list below.
4. **Optional:** Check **Show Latest Event** to view the latest access record.

   The record list will be listed reverse chronologically.
5. **Optional:** Check **Enable Abnormal Temperature Prompt** to enable abnormal skin-surface temperature prompt.

   Note

   When enabled, if there is abnormal temperature information, an Abnormal Temperature window pops up when you enter Monitoring module, displaying person's picture, skin-surface temperature, card No., person name, etc.
6. **Optional:** Click an event to view person pictures (including captured picture and profile).

   Note

   In **Linked Capture Picture** field, you can double click the captured picture to view an enlarged picture.
7. **Optional:** Click ▣ to view details (including person's detailed information and the captured picture).

   Note

   In the pop-up window, you can click □ to view details in full screen.

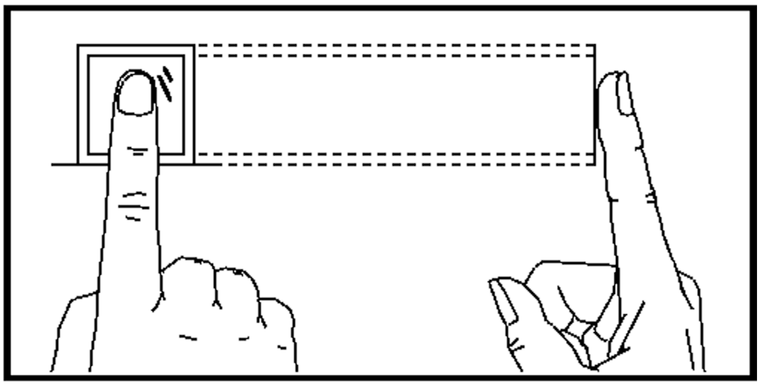
Appendix A. Tips for Scanning Fingerprint

Recommended Finger

Forefinger, middle finger or the third finger.

Correct Scanning

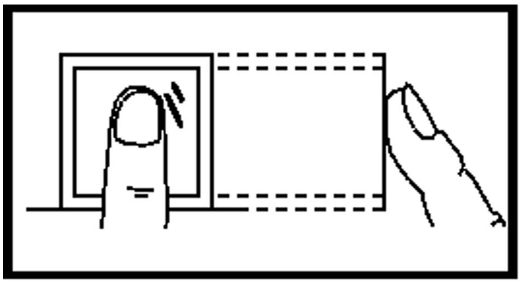
The figure displayed below is the correct way to scan your finger:



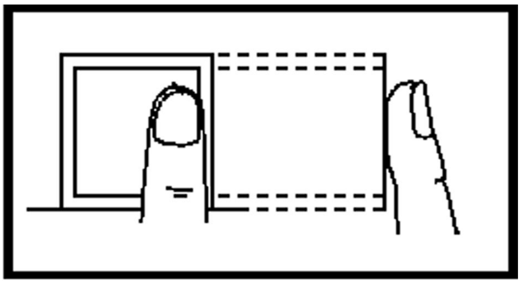
You should press your finger on the scanner horizontally. The center of your scanned finger should align with the scanner center.

Incorrect Scanning

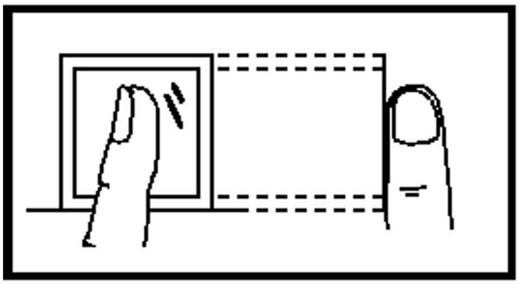
The figures of scanning fingerprint displayed below are incorrect:



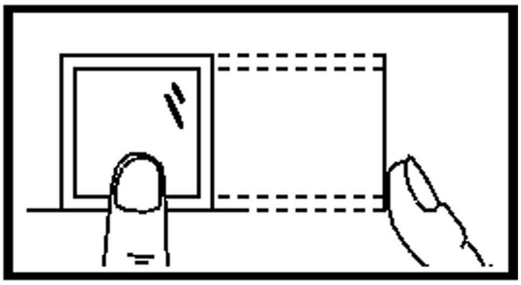
Vertical



Edge I



Side



Edge II

Environment

The scanner should avoid direct sun light, high temperature, humid conditions and rain.
When it is dry, the scanner may not recognize your fingerprint successfully. You can blow your finger and scan again.

Others

If your fingerprint is shallow, or it is hard to scan your fingerprint, we recommend you to use other authentication methods.
If you have injuries on the scanned finger, the scanner may not recognize. You can change another finger and try again.

Appendix B. DIP Switch

B.1 DIP Switch Description

The DIP switch is on the access control board. No.1 and No 2 is from the low bit to the high bit.

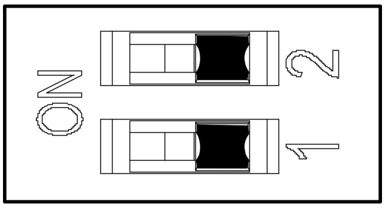


Figure B-1 DIP Switch

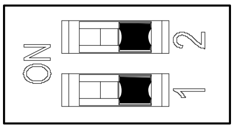
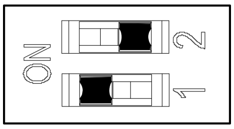
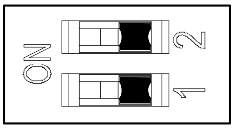
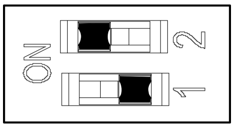
When the switch is towards ON, it means the switch is enabled, otherwise, the switch is off.

B.2 DIP Switch Corresponded Functions

Note

After setting the DIP switch, you should reboot the device, or the function cannot take effect.

The 2-bit DIP switch corresponded functions on the access control board are as follows:

Bit	Device Mode	Function	Decimal Value	DIP Switch Address Diagram
1	Work Mode	Normal Mode	0	
		Study Mode	1	
2	Keyfob Paring Mode	Disable Keyfob Paring Mode	0	
		Enable Keyfob Paring Mode	1	

Appendix C. Error Code Description

The swing barrier will display the error code on the seven-segment display if error occurred. Refer to the table below to find the description of each number.

Error Reason	Code	Error Reason	Code
The First IR Beam Triggered	01	The Eighteenth IR Beam Triggered	18
The Second IR Beam Triggered	02	The Nineteenth IR Beam Triggered	19
The Third IR Beam Triggered	03	The Twentieth IR Beam Triggered	20
The Fourth IR Beam Triggered	04	The Twenty-First IR Beam Triggered	21
The Fifth IR Beam Triggered	05	The Twenty-Second IR Beam Triggered	22
The Sixth IR Beam Triggered	06	The Twenty-Third IR Beam Triggered	23
The Seventh IR Beam Triggered	07	The Twenty-Fourth IR Beam Triggered	24
The Eighth IR Beam Triggered	08	Authentication Indicator Board (Entrance) Offline	49
The Ninth IR Beam Triggered	09	Authentication Indicator Board (Exit) Offline	50
The Tenth IR Beam Triggered	10	IR Adapter Board Offline	51
The Eleventh IR Beam Triggered	11	Interconnecting Exception	53
The Twelfth IR Beam Triggered	12	Not Studying	54
The Thirteenth IR Beam Triggered	13	Obstruction	55
The Fourteenth IR Beam Triggered	14	Exceeding Studying Range	56
The Fifteenth IR Beam Triggered	15	Encoder Exception	57

Error Reason	Code	Error Reason	Code
The Sixteenth IR Beam Triggered	16	Motor Exception	58
The Seventeenth IR Beam Triggered	17	Extended Interface Board Offline (If the board is not installed, the error code of "59" will appear but the device functions normally)	59

Appendix D. Communication Matrix and Device Command

Communication Matrix

Scan the following QR code to get the device communication matrix.
Note that the matrix contains all communication ports of Hikvision access control and video intercom devices.

Figure D-1 QR Code of Communication Matrix

Device Command

Scan the following QR code to get the device common serial port commands.
Note that the command list contains all commonly used serial ports commands for all Hikvision access control and video intercom devices.

Figure D-2 Device Command

See Far, Go Further